Lecture Notes in Computer Science 4217

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Pedro Cuenca Luiz Orozco-Barbosa (Eds.)

Personal Wireless Communications

IFIP TC6 11th International Conference, PWC 2006
Albacete, Spain, September 20-22, 2006
Proceedings

Springer

Volume Editors

Pedro Cuenca
Luiz Orozco-Barbosa
Universidad de Castilla-La Mancha
Departamento de Sistemas Informáticos
Campus Universitario s/n 02071, Albacete Spain
E-mail:{pedro.cuenca,luis.orozco}@uclm.es

Library of Congress Control Number: 2006932620

CR Subject Classification (1998): C.2, H.4, H.3, D.2, K.8

LNCS Sublibrary: SL 5 – Computer Communication Networks and Telecommunications

ISSN 0302-9743
ISBN-10 3-540-45174-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-45174-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11872153 06/3142 5 4 3 2 1 0

Preface

The IFIP TC-6 International Conference on Personal Wireless Communications, PWC, is the main conference of the IFIP Working Group 6.8, Mobile and Wireless Communications. The 11th PWC was held in Albacete, Spain, on September 20-22, 2006. There were 181 submissions from 29 countries, which were evaluated by the program committee members assisted by external reviewers. After a thorough review process, 45 papers were selected to be included in the program. Thus, the acceptance rate was 24 %.

The papers selected in this volume illustrate the state of the art and current trends in the broad area of personal wireless communications. The program was organized into 9 topics:

1. Mobile and Wireless Networking
2. QoS
3. Ad-Hoc
4. Security
5. Wireless LAN
6. Cross-Layer Design
7. Wireless Sensor Networks
8. Physical Layer
9. Mobile and Wireless Applications.

We are grateful to the two keynote speakers, Hari Kalva and Pedro Marron, for accepting our invitation. We would like to thank all the members of the Technical Program Committee and the additional referees. Without their support, the conference organization would not have been possible. Last but not least, we are also grateful to all the authors and participants who trusted us to organize this event and to Springer's LNCS Editorial for supporting us again this year. We expect PWC 2006 to have been a fruitful and stimulating international forum for exchanging ideas and experiences in the area of personal wireless communications.

September 2006

Pedro Cuenca and
Luis Orozco-Barbosa

Organization

General Co-chairs

Pedro Cuenca	Universidad de Castilla-La Mancha, Spain
Luis Orozco-Barbosa	Universidad de Castilla-La Mancha, Spain

Steering Committee

Augusto Casaca	INESC, Portugal
Ramón Puigjaner	Universidad de las Islas Baleares, Spain
Guy Pujolle	University of Paris 6, France
Pedro Cuenca	Universidad de Castilla-La Mancha, Spain
Ivan Stojmenovic	University of Ottawa, Canada
Luis Orozco-Barbosa	Universidad de Castilla-La Mancha, Spain
Ottio Spaniol	University of Technology of Aachen, Germany
Guy Omidyar	Consultant, USA
Jan Slavik	TESTCOM, Czech Republic

Organizing Committee

Pedro Cuenca	Universidad de Castilla-La Mancha, Spain
Francisco Delicado	Universidad de Castilla-La Mancha, Spain
Jesús Delicado	Universidad de Castilla-La Mancha, Spain
Gerardo Fernandez	Universidad de Castilla-La Mancha, Spain
Raúl Galindo	Universidad de Castilla-La Mancha, Spain
Antonio Garrido	Universidad de Castilla-La Mancha, Spain
Jose Luis Martínez	Universidad de Castilla-La Mancha, Spain
Francisco Mico	Universidad de Valencia, Spain
Teresa Olivares	Universidad de Castilla-La Mancha, Spain
Luis Orozco-Barbosa	Universidad de Castilla-La Mancha, Spain
Francisco José Quiles	Universidad de Castilla-La Mancha, Spain
José Villalón	Universidad de Castilla-La Mancha, Spain

Technical Program Committee

Dharma P. Agrawal	University of Cincinnati, USA
Raffaele Bruno	IIT-CNR, Italy
Augusto Casaca	INESC, Portugal
Amitabha Das	Nanyang Technological University, Singapore
Francisco M. Delicado	Universidad de Castilla-La Mancha, Spain

Luigi Fratta	Politecnico di Milano, Italy
Rajit Gadh	UCLA, USA
Javier Garcia	Universidad Complutense de Madrid, Spain
Jorge Garcia	Universidad Politécnica de Cataluña, Spain
Silvia Giordano	ICA-DSC-EPFL, Switzerland
Takeshi Hattori	Sophia University, Japan
Sonia Heemstra de Groot	Ericsson EuroLab, The Netherlands
Villy Baek Iversen	Technical University of Denmark, Denmark
Ahmed Kamal	Iowa State University, USA
Ousmane Koné	Université Paul Sabatier - IRIT, France
Hyong W. Lee	Korea University, Korea
Victor Leung	University of British Columbia, Canada
Miguel López	Universidad Autónoma Metropolitana, Mexico
Pascal Lorenz	University of Haute Alsace, France
Zoubir Mammeri	University of Toulouse, France
Vicenzo Mancuso	University of Palermo, Italy
Pietro Manzoni	Universidad Politécnica de Valencia, Spain
Ali Miri	University of Ottawa, Canada
Ignacious Niemegeers	Delft University, The Netherlands
Guy Omidyar	Consultant, USA
Stephan Olariu	Old Dominion University, USA
Teresa Olivares	Universidad de Castilla-La Mancha, Spain
Manuel Perez Malumbres	Universidad Miguel Hernández, Spain
Samuel Pierre	Ecole Polytechnique du Montreal, Canada
Ramón Puigjaner	Universidad de las Islas Baleares, Spain
Fernando Ramirez	ITAM, Mexico
Pedro Ruiz	Universidad de Murcia, Spain
Guy Pujolle	University of Paris 6, France
Pierre R. Chevillat	IBM Zurich Research Laboratory, Switzerland
Debashis Saha	Indian Institute of Management (IIM), India
Jun-Bae Seo	ETRI, Korea
Jan Slavik	TESTCOM, Czech Republic
Ottio Spaniol	University of Technology of Aachen, Germany
Dirk Staehle	University of Wuerzburg, Germany
Ivan Stojmenovic	University of Ottawa, Canada
Samir Tohme	ENST, France
Luis Villaseñor	CICESE, Mexico
Jozef Wozniak	Technical University of Gdansk, Poland

Invited Lectures

Hari Kalva	Florida Atlantic University, USA
Pedro Marrón	University of Stuttgart, Germany

Referees

Dharma P. Agrawal
Raúl Aquino
Robert Bestak
Raffaele Bruno
Augusto Casaca
Pierre R. Chevillat
Pedro Cuenca
Francisco M. Delicado
Jesús Delicado
Amitabha Das
Diego Dujoune
Luigi Fratta
Rajit Gadh
Javier Garcia
Jorge Garcia
Francisco García-Ugalde
Antonio Garrido
Silvia Giordano
Javier Gomez
Takeshi Hattori
Sonia Heemstra de Groot
Villy Baek Iversen
Ahmed Kamal
Ousmane Koné
Hyong W. Lee
Ki-Dong Lee
Victor Leung
Miguel López
Pascal Lorenz
Zoubir Mammeri
Vicenzo Mancuso
Pietro Manzoni
Francisco Micó
Ali Miri
Ignacious Niemegeers
Guy Omidyar
Stephan Olariu
Teresa Olivares
Luis Orozco-Barbosa
Paulo Pereira
Manuel P. Malumbres
Samuel Pierre
Ramón Puigjaner
Guy Pujolle
Francisco José Quiles
Victor M. Ramos
Fernando Ramirez
Pedro Ruiz
Miguel Ruiz-Sanchez
Debashis Saha
Jun-Bae Seo
Yongho Seok
Jan Slavik
Ottio Spaniol
Dirk Staehle
Ivan Stojmenovic
Samir Tohme
José Villalón
Luis Villaseñor
Jeong-Joe Won
Jozef Wozniak
Zhanping Yin

Sponsoring Institutions

DSI: Departamento de Sistemas Informáticos, UCLM
EPSA: Escuela Politécnica Superior de Albacete
I3A: Instituto de Investigación en Informática de Albacete
PCyTA: Parque Científico y Tecnológico de Albacete
UCLM: Universidad de Castilla-La Mancha
JCCM: Junta de Comunidades de Castilla-La Mancha
MEC: Ministerio de Educación y Ciencia

Table of Contents

Mobile and Wireless Networking

QoS

Ad-Hoc (I)

Security

Ad-Hoc (II)

Wireless LAN

Cross-Layer Desing

Wireless Sensor Networks (I)

Physical Layer

Wireless Sensor Networks (II)

Mobile and Wireless Applications

Mobility Protocols for Handoff Management in Heterogeneous Networks

F. Siddiqui[1] and S. Zeadally[2]

[1] Wayne State University, Detroit, MI 48202, USA
[2] University of the District of Columbia, Washington, DC 20008 USA

Abstract. Future generation networks are expected to be a combination of several types of access technologies that vary in their characteristics. Efficient handoff management techniques are required to enable end-users to seamlessly access these networks as they roam across different geographic locations. We describe recent protocols (application, transport, and network) such as Mobile IP, Session Initiation Protocol (SIP), and Stream Control Transmission Protocol (SCTP) that have been deployed to handle handoffs. We present an empirical performance evaluation of the three protocols using performance metrics such as handoff delay. We found that Mobile IP yields the highest handoff delay out of all the three mobility protocols. SIP and SCTP yield (33 %) and (55 %) lower handoff delays compared to Mobile IP.

Keywords: Handoff, Mobility, Heterogeneous, Protocols, Networks.

1 Introduction

The demand for ubiquitous information access has led to the convergence of several types of networks including Ethernet Local Area Network (LAN), General Packet Radio Service (GPRS), Global System for Mobile Communication (GSM), Wireless Local Area Network (WLAN), Bluetooth, etc. In such heterogeneous environments mobility management is the basis for providing continuous network connectivity to mobile users roaming between these access networks. There are two major components of mobility management: Location management and Handoff management. Location management enables the network to discover the current attachment point of the mobile user. Handoff management enables the mobile node to maintain the network connection as it continues to move and change its access points or base stations to the network.

Several protocols have been proposed [9] [10 [11] to address the issue of mobility management in heterogeneous networks. These approaches operate at different levels of the network protocol stack.

- ***Network Layer:*** Mobile IP [1] was proposed by the Internet Engineering Task Force (IETF) to handle mobility management at the network layer. It handles mobility by redirecting packets from a mobile node's home network to the mobile node's current location. Deployment of Mobile IP requires network servers including a home agent and a foreign agent that are used to bind the home address

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 1 – 12, 2006.

of a Mobile Node (MN) to the care-of address at the visited network and provide packet forwarding when the MN is moving between IP subnets.

- ***Application Layer:*** The Session Initiation Protocol (SIP) [2] is an application layer protocol that keeps mobility support independent of the underlying access technologies. In the SIP approach, when an MN moves during an active session into a different network, it first receives a new network address, and then sends a new session invitation to the correspondent node. Subsequent data packets from the CN are forwarded to the MN using the new address. The MN also needs to register its new IP address with a SIP server called a Registrar to enable other nodes on the network to reach it by querying the Registrar server.
- ***Transport Layer:*** A third approach for mobility management has been proposed at the transport layer in the form of the Stream Control Transmission Protocol (SCTP) [3]. The SCTP-based approach uses multihoming for implementing mobility management. The multihoming feature allows a SCTP to maintain multiple IP addresses. Among those addresses, one address is used as the primary address for current transmission and reception. Other addresses (secondary) can be used for retransmissions. The multihoming feature of SCTP provides a basis for mobility support since it allows a mobile node (MN) to add a new IP address, while holding an old IP address already assigned to it.

In this paper we present a comparison of SIP, Mobile IP and SCTP for supporting handoff management in heterogeneous networks. We present an empirical evaluation of handoff latency achieved in the case of each protocol when a mobile user roams across different types of networks. We also identify issues in setting up a testbed to conduct handoff delay tests. The rest of this paper is organized as follows. In section 2 we give an overview of the three mobility management protocols: SIP, Mobile IP, and SCTP. Section 3 discusses the experimental procedures and testbed setup used for conducting our performance evaluation tests. In section 4 we present a performance analysis of handoffs conducted across different network types. Finally, in section 5 we make some concluding remarks.

2 Mobility Management Protocols

2.1 SIP-Based Terminal Mobility

SIP is an application-layer control protocol that can establish, modify and terminate multimedia sessions [2]. SIP defines several logical entities, namely user agents, redirect servers, proxy servers and registrars. SIP inherently supports personal mobility and can be extended to support service and terminal mobility [8]. Terminal mobility allows a device to move between IP sub-nets, while continuing to be reachable for incoming requests and maintaining sessions across subnet changes. Mobility of hosts in heterogeneous networks is managed by using the terminal mobility support of SIP.

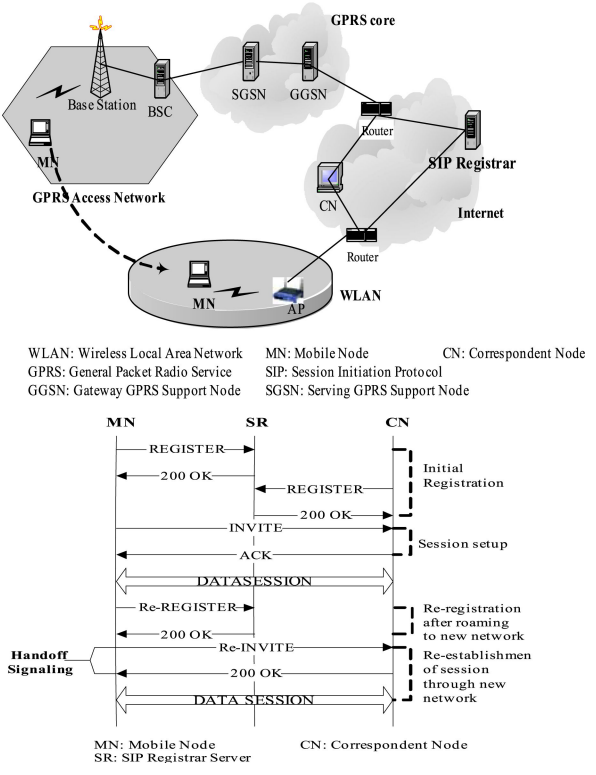


Fig. 1. SIP-based Mobility Management

Terminal mobility requires SIP to establish a connection either during the start of a new session, when the terminal or MN has already moved to a different location, or in the middle of a session. The former situation is referred to as *pre-call mobility*, latter as *mid-call* or *in-session mobility*. For pre-call mobility, the MN re-registers its new IP address with the Registrar server by sending a REGISTER message, while for mid-call mobility the terminal needs to notify the correspondent Node (CN) or the host communicating with the MN by sending a re-INVITE message about the terminal's new IP address and updated session parameters. The CN starts sending data to the new location as soon as it receives the re-INVITE message. The MN also needs to register with the redirect server in the home network for future calls. Figure 1 shows the messages exchanged for setting up a session between a mobile node and a correspondent node and continuing it after changing the access network.

2.2 Mobile-IP-Based Mobility

Mobile IP is a mobility management protocol proposed to solve the problem of node mobility by redirecting packets to the mobile node's current location. The Mobile IP

architecture is shown in figure 2. Its main components include a Home Agent (HA) and a Foreign Agent (FA). HA is a router on a mobile node's home network, which encapsulates datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node. FA is a router on a mobile node's visited network (foreign network) that provides routing services to the mobile node when registered. The FA decapsulates and delivers datagrams, tunneled by the mobile node's HA to the mobile node. When a mobile node moves out of its home network it must obtain another IP. So, in Mobile IP, a mobile host uses two IP addresses: a fixed home address (a permanent IP address assigned to the host's network) and a *care-of-address* - a temporary address from the new network (i.e. foreign network) that changes at each new point of attachment. When the mobile node moves, it has to first discover its new care-of-address. The care-of-address can be obtained by periodic advertising from the FA through broadcasting. The mobile node then registers its care-of-address with its home agent by sending a Registration Request to its home agent via the foreign agent. The HA then sends a Registration Reply either granting or denying the request. If the registration process is successful, any packets destined for the MN are intercepted by the HA, which encapsulates the packets and tunnels them to the FA where decapsulation takes place and the packets are then forwarded to the appropriate MN.

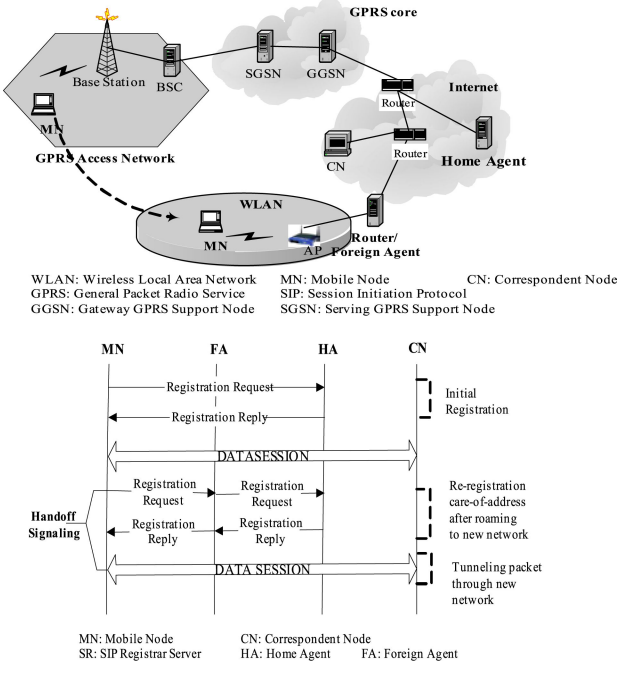


Fig. 2. Mobile-IP-based Mobility Management

2.3 SCTP Based Mobility

The Stream Control Transmission Protocol (SCTP) [3] is a reliable connection-oriented transport protocol that operates over a potentially unreliable connectionless packet service, such as IP. Before peer SCTP users can send data to each other, a connection must be established between two endpoints. This connection is called an association in SCTP context. A cookie mechanism is employed during the initialization of an association to provide protection against security attacks. Figure 3 shows a sample SCTP message flow. An essential property of SCTP is its support for multihomed nodes, i.e. nodes that can be reached under several IP addresses. If a client is multi-homed, it informs the server about all its IP addresses with the INIT chunk's address parameters. An extension to the SCTP called mSCTP (Mobile SCTP) also allows dynamic addition and deletion of IP addresses from an association, even if these addresses were not present during association startup. This feature of SCTP is used to support mobility of hosts across different networks.

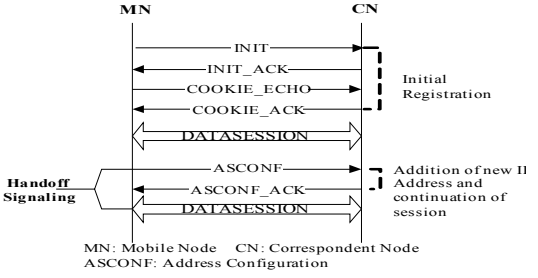


Fig. 3. SCTP-based Mobility Management

3 Performance Evaluation of Mobility Protocols

3.1 Experimental Testbed

We conducted experimental measurements to determine the handoff delay experienced while roaming across different networks. The handoff tests were conducted for each of the mobility protocols: SIP, Mobile IP, and SCTP.

Figure 4 shows the experimental testbed used for conducting the handoff measurements. The setup consists of a DELL laptop (client machine) equipped with three network interface cards (NICs): a built-in Natsemi Ethernet NIC (100 Mbps), a built-in Orinoco WLAN NIC (11 Mbps) and an external PCMCIA GPRS Sierra Wireless aircard 750 (144 Kbps). The Ethernet interface (eth0) of the client machine is connected to a 100 Mbits/sec switch that connects to the external IP network (Internet). The WLAN interface (eth1) of the client machine is associated with a WLAN access point, which is in turn connected to the router for Internet access. The GPRS interface (ppp0) is associated with a T-Mobile GPRS base station, which connects to the Internet via the GPRS core network. In order to use the GPRS

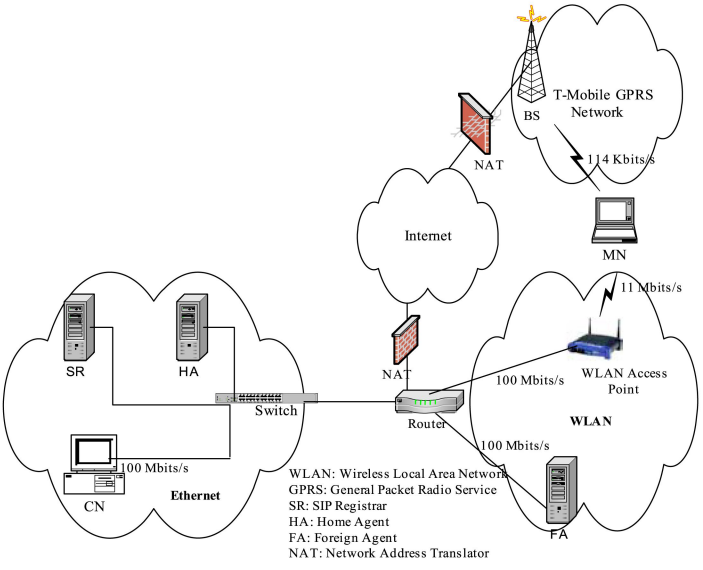


Fig. 4. Experimental Testbed used for SIP, Mobile IP, and SCTP Handoff Performance Measurements

network, we purchased a GPRS data plan subscription from the T-Mobile service provider [5]. Other components of the testbed include a SIP Registrar server, a Home Agent, and a Foreign Agent.

The client (Mobile Node) and the server (Correspondent Node) machines were loaded with Redhat 9.0 Linux operating system and used a kernel version of 2.4.20-8. For SCTP-based mobility tests, a user-level implementation of SCTP called Sctplib-1.3.1 [6] (developmental version) was used. For Mobile-IP-based tests, a Mobile IP user-level implementation called Dynamics [7] from Helsinki University of Technology was used. SIP-based mobility was tested by implementing a simple SIP user-agent client [8], a SIP user agent server and a SIP Registrar server using the SIP methods (INVITE, ACK, BYE, REGISTER, and CANCEL) described in RFC 3261 [2].

3.2 Measurement Procedures and Performance Metrics

We measured the handoff delay experienced when roaming across three types of networks: Ethernet, WLAN and GPRS by implementing mobility protocols at the application (SIP), network (Mobile IP) and Transport (SCTP) layers.

In the case of SIP, we measured the handoff delay experienced by a mobile node in six different cases:

- GPRS to WLAN
- WLAN to GPRS
- Ethernet to WLAN

- WLAN to Ethernet
- Ethernet to GPRS
- GPRS to Ethernet

In the case of SCTP and Mobile IP, we measured the handoff delay in two different cases:

- Ethernet to WLAN
- WLAN to Ethernet

The performance metrics that we measured are as follows:

- ***Total Handoff Delay:*** The total handoff delay is the time difference between the last data packet received at the old network interface and the first data packet received on the new network interface. The total handoff delay includes the handoff time as well as the time taken for the first data packet to arrive from the mobile node to the correspondent node.
- ***Handoff Signaling Time:*** The handoff signaling time is a measure of the time required to exchange signaling messages to execute a handoff. The number of signaling messages exchanged is different for each mobility management protocol.
- ***Packet Transmission Delay after handoff:*** The packet transmission delay after the handoff is a measure of the transmission time of a packet from the mobile node to the correspondent node after the mobile node has moved to a new network.

3.2.1 SCTP and Mobile IP Issues for NAT Traversal

It was not possible to measure the handoff delay (for SCTP and Mobile IP) while moving from the GPRS network to the other networks (Ethernet and WLAN) and vice versa because the GPRS operator assigns a dynamic, private IP address to the mobile node. A dynamic IP address is one that is not manually specified and is not a permanent address. It is a temporary address that is dynamically configured using the Dynamic Host Configuration Protocol (DHCP). A private IP address is one that can be used by any machine and is therefore re-usable. However, private IP addresses are not routable over the public Internet. They are used in private networks due to the shortage of public, routable IP addresses. The range of IP addresses reserved for private use includes 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255. Also, each Internet provider network employs a Network Address Translator (NAT) for providing Internet access to the internal nodes with private IPs and also for security purposes.

The problem with Dynamics implementation of Mobile IP is that it is not "NAT traversal" capable. When a mobile node moves to the GPRS network, it acquires a care-of-address (CoA), which is a private address. Then the mobile node sends a Registration Request to the Home Agent (HA) to register its new CoA. However, at the NAT gateway, the private IP address of this packet (source IP address in the IP header) is replaced by the public IP address of the NAT gateway. When the

Registration Request arrives at the HA, the HA detects that that the source address of the packet (which is the public address) is different from the CoA inside the Registration Request message (present in the Mobile IP header). Therefore the HA drops the request. Thus, in the case of the Dynamics, it is necessary to have a public, static IP address for the mobile node. Hence, handoffs involving the GPRS network could not be tested due to the assignment of a private IP.

In the case of SCTP, when the mobile node is located in the GPRS network and the correspondent node is located on a different network, all packets from the mobile node have to pass through the NAT. SCTP has certain issues related to NATs. If Network Address Port Translation is used with a multihomed SCTP endpoint, then any port translation must be applied on a per-association basis such that an SCTP endpoint continues to receive the same port number for all messages within a given association. The NAT needs to understand this requirement to allow mobility support using SCTP. Since existing NATs are not designed to support SCTP, a NAT assigns a different port number when the SCTP association changes its primary address. The SCTP server does not accept the change in the port number and breaks the association. Thus SCTP cannot be experimented with a GPRS network employing a NAT that is not configured to support SCTP.

4 Experimental Results and Discussion

In this section we present an analysis of the handoff performance obtained for the three mobility management protocols. Figure 5 shows the total handoff delay obtained while roaming from Ethernet to WLAN and vice versa using SIP, Mobile IP and SCTP. It is worthwhile mentioning that SIP, Mobile IP and SCTP operate at the application, network, and transport layers respectively.

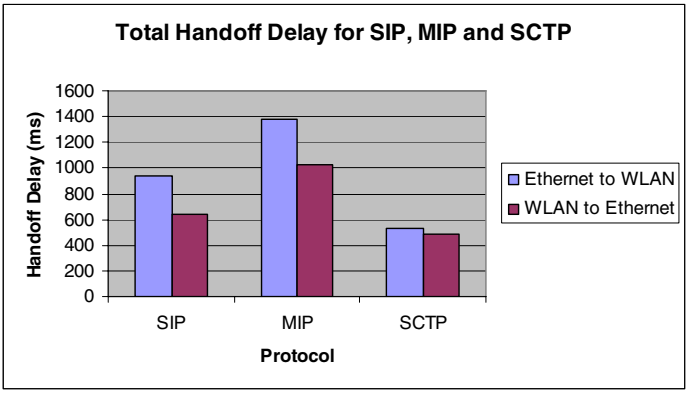


Fig. 5. Total Handoff Delay for SIP, Mobile IP and SCTP

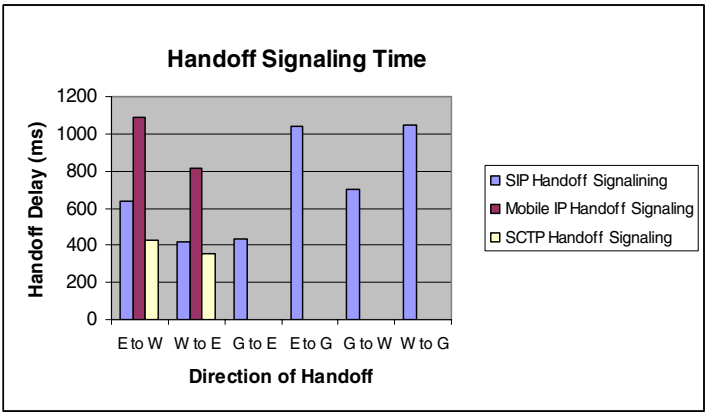


Fig. 6. Handoff Signaling Time for SIP, Mobile IP, and SCTP

It can be observed from figure 5 that the total handoff delay in either direction (Ethernet to WLAN and vice versa) is the lowest in the case of SCTP followed by SIP and is the highest in the case of Mobile IP. The total handoff delay is lowest for SCTP (31% lower compared to SIP and 55% lower compared to Mobile IP for WLAN to Ethernet handoff). The reason for the low handoff delay in the case of SCTP is because the SCTP client immediately adds the IP address of a newly discovered network to its list of available networks and also relays this information to the SCTP server. When a handoff is initiated due to the unavailability of the current network, the client sends an ASCONF_DELETEIP message to the server (for removing the old IP address) and starts using the interface with the new IP address for data transmission. Thus, the handoff process with SCTP involves very few signaling messages thereby resulting in a low total handoff time. Table 1 lists the signaling messages exchanged for implementing handoffs using SIP, Mobile IP and SCTP.

Table 1. Components of Handoff Signaling: SIP, Mobile IP, and SCTP

Protocol	Handoff Messages
SIP	Re-Register
	ACK
Mobile IP	Registration Request,
	Registration Reply
SCTP	ASCONF_DELETE IP

In the case of SIP, when a handoff is initiated, the SIP client sends a Re-INVITE message to the SIP server using the new interface. After the SIP server acknowledges the Re-INVITE, the communication between the client and the server is continued. Thus, handoff delay in the case of SIP is the two-way delay involved in sending the Re-INVITE message and receiving an acknowledgement. We determine the handoff

delay at the correspondent node as the time difference between the last data packet received at the old network interface and the first data packet received at the new network interface. Thus, the handoff delay also includes the transmission time of the first packet following the handoff signaling. In the case of Mobile IP, the handoff involves a higher number of signaling messages compared to SIP and SCTP. Mobile IP requires the mobile node needs to send a Registration Request to the Foreign Agent that forwards the request to the Home Agent. The Registration Reply is sent by the Home Agent to the Foreign Agent which then gets forwarded to the mobile node. Due to the high signaling overhead involved in the case of handoffs based on Mobile IP, the signaling time is also higher.

Figure 6 shows the handoff signaling time in the case of the SIP protocol when the mobile node moves across various networks. It can be observed that the signaling time is the highest when the mobile node makes a handoff to a GPRS network. The signaling time is comparatively lower when the mobile moves to the WLAN and is the lowest in the case of transition to an Ethernet network. We note that the low signaling delay associated with transition to an Ethernet network is probably because of Ethernet's lowest transmission latency. To confirm this explanation, we performed a simple test using Netperf [4] to determine the available bandwidth and the latency offered by each of these networks. As shown in table 2, the latency incurred on the GPRS network is comparatively higher as compared to Ethernet and WLAN. This accounts for the high handoff signaling delay when the mobile node moves to the GPRS network. We also observe (from figure 6) that there is a 41 % reduction in the handoff signaling time in the case of SIP when compared to Mobile IP (for handoff to a WLAN) and a 60 % decrease in the handoff signaling time in the case of SCTP as compared to Mobile IP.

Table 2. Network Characteristics determined by running a Netperf test

Network Type	Link Speed	Actual Measured Bandwidth	Average Latency (one-way)
GPRS	114 Kbps	28.9 Kbps	891 ms
WLAN	11 Mbps	5.51 Mbps	61 ms
Ethernet	100 Mbps	88.8 Mbps	36 ms

Figure 7 shows the transmission delay incurred by packets arriving at the correspondent node after the handoff. We observe that in the case of Mobile IP, we obtained highest packet transmission delay. As observed from figure 7, there is a 47 % decrease in the packet transmission delay in the case of SIP as compared to Mobile IP (in the case of handoff to a WLAN) and a 54 % decrease in the packet transmission delay with SCTP as compared to Mobile IP (in the case of handoff to a WLAN). This is because, after handoff, packets from the Mobile Node to the Correspondent Node have to be routed through the Home Agent and the Foreign Agent before they can reach the Correspondent Node. This introduces additional delay in the transmission time. The packet transmission delay for SCTP and SIP is almost the same. In both these cases, the packets following handoff are sent directly from the Mobile Node to the Correspondent Node. This results in a lower packet transmission delay for SIP and SCTP as compared to Mobile IP.

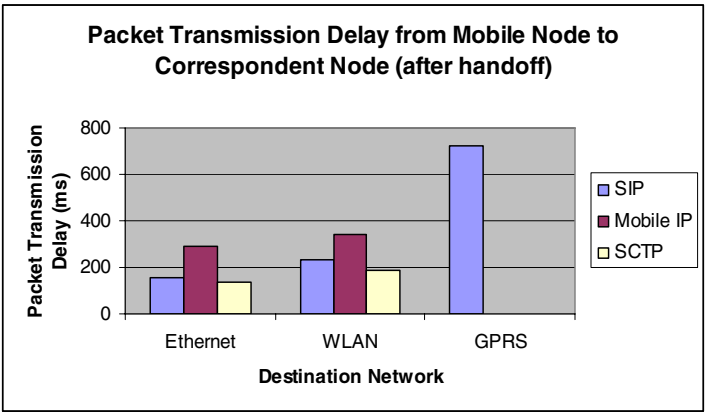


Fig. 7. Packet Transmission Delay after Handoff

5 Conclusions and Future Work

In this paper we have compared the handoff performance of three types of mobility management protocols: SIP, Mobile IP and SCTP. We found that SCTP performs well both, in terms of handoff delay, as well as the packet transmission time after a handoff. The SIP protocol incurred a higher handoff delay compared to SCTP but the packet transmission time for packets after a handoff was almost comparable for the two protocols. Mobile IP showed higher handoff delay as well as longer packet transmission time following handoff to a new network. However, Mobile IP keeps the change in the IP address completely transparent to the other end-system. In the case of SIP and SCTP, the change in the destination IP address has to be conveyed to the node at the other end. SCTP-based mobility is however completely transparent to the application, whereas in the case of SIP, applications need to be aware of mobility.

We also discussed the issues that exist in connection with deploying Mobile IP and SCTP over networks using private IP addresses and deploying NATs. Mobile IP and SCTP are not capable of operating in networks with NAT mechanisms. Since almost all network operators use NATs in their networks, it is crucial to extend these protocols to enable them to operate across heterogeneous domains. One method that can be used is to enable this feature is to use UDP encapsulation in each of these protocols. Since most NATs are already designed to provide support for UDP packets, encapsulating SCTP packets inside UDP can make SCTP operate across NATs belonging to different network domains. However, this would introduce additional encapsulation-decapsulation delays. In our future work, we aim at overcoming the drawbacks of these protocols and design a solution for handoff management that is not specific to a single layer of the network protocol stack, but employs a cross-layer design for achieving seamless handoffs across heterogeneous networks. We plan to implement a mobility middleware that performs handoffs using the information from various layers (such as link quality information from layer 2, QoS information from layer 4, etc) of the protocol stack and is deployable across existing network configurations.

References

1. C. Perkins, “Mobile networking through Mobile IP”, IEEE Internet Computing, Volume 2, Issue 1, January - February 1998 Pages: 58 – 69.
2. Rosenberg et al., “Session Initiation Protocol”, RFC 3261.
3. Stewart et al., “Stream Control Transmission Protocol”, RFC 2960.
4. Netperf, http://www.netperf.org
5. T-Mobile, http://www.tmobile.com
6. SCTP Implementation, http://www.sctp.de
7. Mobile IP, Dynamics Implementation, http:// www.cs.hut.fi/Research/Dynamics
8. Schulzrinne H., “Application Layer Mobility with SIP”, ACM SIGMOBILE Mobile Computing and Communications, Volume 4, Issue 3, July 2000, Pages: 47 – 57.
9. Eddy, W., “At What Layer Does Mobility Belong”, IEEE Communications Magazine, Volume 42, Issue 10, October 2004 Pages: 155 – 159.
10. Chiussi, F.M.; Khotimsky, D.A.; Krishnan, S, “Mobility management in third-generation all-IP networks”, IEEE Communications Magazine, Volume 40, Issue 9, September 2002 Pages:124 – 135.
11. Banerjee, N.; Das, S.K.; Acharya, A., “SIP-Based Mobility Architecture for Next Generation Wireless Networks”, in proceedings of the third IEEE International Conference on Pervasive Computing and Communications, 8-12 March 2005 Pages:181 – 190.

Supporting Group Communication in WCDMA Networks

Antonios Alexiou, Dimitrios Antonellis, and Christos Bouras

Research Academic Computer Technology Institute, N. Kazantzaki str,
26500 Patras, Greece and
Computer Engineering and Informatics Department,
University of Patras, 26500 Patras, Greece
alexiua@cti.gr, antonel@cti.gr, bouras@cti.gr

Abstract. It is known that multicast is an efficient method of supporting group communication as it allows the transmission of the packets to multiple destinations using fewer network resources. Along with the widespread deployment of the third generation cellular networks and the fast-improving capabilities of the mobile devices, content and service providers are increasingly interested in supporting multicast communications over wireless networks and in particular over Universal Mobile Telecommunications System (UMTS). In this paper, a multicast scheme for UMTS is analyzed. We analytically present the multicast routing mechanism behind our scheme as well as the multicast group management functionality of the scheme. Furthermore, we present an evaluation of our scheme in terms of its performance. The critical parameters for the evaluation of the scheme are the number of users within the multicast group, the amount of data sent to the multicast users, the density of the multicast users within the cells and finally the type of transport channel used for the transmission of the multicast data over the air.

1 Introduction

UMTS constitutes the third generation of cellular wireless networks which aims to provide high-speed data access along with real time voice calls. Wireless data is one of the major boosters of wireless communications and one of the main motivations of the next generation standards [9]. The multicast transmission of real time multimedia data is an important component of many current and future emerging Internet applications, such as videoconference, distance learning and video distribution. It offers efficient multidestination delivery, since data is transmitted in an optimal manner with minimal packet duplication [10], [11].

Compared with multicast routing in the Internet, mobile networks such as UMTS pose a very different set of challenges for multicast. First, multicast receivers are nonstationary and consequently may change their point of attachment to the network at any given time. Second, mobile networks are generally based on a well-defined tree topology, with the nonstationary multicast receivers being located at the leaves of the network tree. It is therefore not appropriate to apply conventional IP multicast routing mechanisms in UMTS, since they cannot manage the mobility of the mobile users [2].

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 13 – 24, 2006.

Several multicast mechanisms for UMTS have been proposed in the literature. In [1], the authors discuss the use of commonly deployed IP multicast protocols in UMTS networks. However, in [2] the authors do not adopt the use of IP multicast protocols for multicast routing in UMTS and present an alternative solution. More specifically, in order to overcome the one-to-one relationship between a single subscriber and a GPRS Tunneling Protocol (GTP) tunnel that is inherent to the hierarchical routing in UMTS, they implement a Multicast-Packet Data Protocol (M-PDP) context for each multicast group in the GGSN and SGSN. Furthermore in [3], a multicast mechanism for circuit-switched GSM and UMTS networks is outlined, while in [4] an end-to-end multicast mechanism for software upgrades in UMTS is analyzed. Additionally, the 3rd Generation Partnership Project (3GPP) is currently standardizing the Multimedia Broadcast/Multicast Service (MBMS) [5], [12].

In this paper, we analytically present a multicast scheme for UMTS. The multicast routing mechanism behind our scheme is analyzed as well as the multicast group management functionality of our mechanism. Additionally, we analyze the performance of the scheme, in terms of the packet delivery cost and the scalability of the scheme, considering different transport channels for the transmission of the multicast data over the air. These channels include the Dedicated Channel (DCH) and a common transport channel such as the Forward Access Channel (FACH). Furthermore, we propose methods that may reduce the packet delivery cost of the multicast data and improve the performance of the delivery scheme. A preliminary version of this paper has been presented in [13] as a poster.

The paper is structured as follows. In Section 2 we provide an overview of the UMTS. Section 3 presents a multicast scheme for UMTS. Following this, Section 4 analyzes the cost of this scheme in function of a number of parameters, while Section 5 presents some numerical results that characterize the multicast scheme. Finally, some concluding remarks and planned next steps are briefly described.

2 Overview of the UMTS in the Packet Switched Domain

A UMTS network consists of two land-based network segments: the core network (CN) and the UMTS Terrestrial Radio-Access Network (UTRAN) (Fig. 1). The CN is responsible for the routing of the calls and the data connections to the external networks, while the UTRAN handles all radio-related functionalities. The CN consists of two service domains: the circuit-switched (CS) service domain and the Packet-Switched (PS) service domain. The CS domain provides access to the PSTN/ISDN, while the PS domain provides access to the IP-based networks. In the remainder of this paper, we will focus on the UMTS packet-switching mechanism. The Packet-Switched (PS) portion of the CN in UMTS consists of two General Packet Radio Service (GPRS) support nodes (GSNs), namely the gateway GPRS support node (GGSN) and the Serving GPRS Support Node (SGSN) (Fig. 1). An SGSN is connected to the GGSN via the Gn interface and to UTRAN via the Iu interface. The UTRAN consists of the Radio Network Controller (RNC) and Node B, which constitutes the base station and provides radio coverage to a cell. Node B is connected to the User Equipment (UE) via the Uu interface (based on the WCDMA technology) and to the RNC via the Iub interface. The GGSN interacts with external Packet Data

Networks (PDNs) through the Gi interface. The GGSN is like an edge IP router providing connectivity with IP networks. The Broadcast/Multicast Service Center (BM-SC) serves as the entry point of data delivery for internal sources and it is introduced in Release 6 of UMTS [9]. In the UMTS PS domain, the cells are grouped into Routing Areas (RAs), while the cells in an RA are further grouped into UTRAN Registration Areas (URAs) [7].

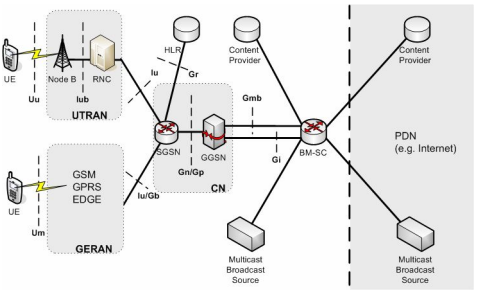


Fig. 1. UMTS architecture

Before a UE can exchange data with an external PDN, the UE must first establish a virtual connection with this PDN. Once the UE is known to the network, packets are transferred between the UE and the network, based on the Packet Data Protocol (PDP), the network-layer protocol carried by UMTS. An instance of a PDP type is called a PDP context and contains all the parameters describing the characteristics of the connection to an external network by means of end-point addresses and QoS. A PDP context is established for all the application traffic sourced from and destined for one IP address. A PDP context activation is a request–reply procedure between a UE and the GGSN. A successful context activation leads to the creation of two GPRS Tunneling Protocol (GTP) sessions, specific to the subscriber: between the GGSN and SGSN over the Gn interface and between the SGSN and RNC over the Iu interface. IP packets destined for an application using a particular PDP context are augmented with UE- and PDP-specific fields and are tunneled using GTP to the appropriate SGSN. The SGSN recovers the IP packets, queries the appropriate PDP context based on the UE- and PDP-specific fields and forwards the packets to the appropriate RNC. The RNC maintains Radio-Access Bearer (RAB) contexts. Equivalently to PDP contexts, a RAB context allows the RNC to resolve the subscriber identity associated with a GTP-tunneled network packet data unit. The RNC recovers the GTP-tunneled packet and forwards the packet to the appropriate Node B [2], [8].

In the remainder of this section, we present a short description of the MBMS framework of the UMTS. It consists of a MBMS bearer service and a MBMS user service. The latter represents applications, which offer for example multimedia content to the users, while the MBMS bearer service provides means for user authorization, charging and QoS improvement to prevent unauthorized reception [12]. The major modification in the existing GPRS platform is the addition of a new entity called BM-SC (Fig. 1). As the term Multimedia Broadcast/Multicast Service

indicates, there are two types of service modes: the broadcast and the multicast mode. Since the multicast mode is more complicated than the broadcast mode, it is more useful to present the operation of the MBMS multicast mode and the way that the mobile user receives the multicast data of a service. Thus, the actual procedure of the reception of an MBMS multicast service is enabled by certain procedures that are illustrated in Fig. 2. The phases Subscription, Joining and Leaving are performed individually per user. The other phases are performed for a service, i.e. for all users interested in the related service. The sequence of the phases may be repeated, depending on the need to transfer data. Also Subscription, Joining, Leaving, Service Announcement, as well as MBMS notification may run in parallel to other phases [12].

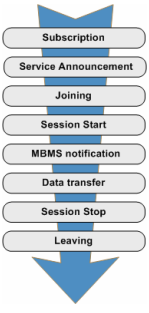


Fig. 2. Phases of MBMS multicast service provision

3 A Multicast Approach for UMTS

In this section we present an overview of a multicast scheme for UMTS. More specifically, it is presented in detail the way that the multicast packets are delivered to a group of mobile users. Additionally, we analyze the packet forwarding / routing mechanism behind the multicast scheme as well as the multicast group management functionality of the scheme.

Fig. 3 shows a subset of a UMTS network. In this architecture, there are two SGSNs connected to an GGSN, four RNCs, and twelve Node Bs. Furthermore, eleven members of a multicast group are located in six cells. The BM-SC acts as the interface towards external sources of traffic [5]. In the presented analysis, we assume that a data stream coming from an external PDN through BM-SC, must be delivered to the eleven UEs as illustrated in Fig. 3.

For the efficient multicast packet forwarding mechanism, every node of the network (except the UEs) maintains a Routing List (Fig.4a). In this list of each node, we record the nodes of the next level that the messages for every multicast group should be forwarded. Additionally, we keep information regarding the QoS profile of the specific multicast group. This information is useful for congestion avoidance and rate control. Obviously, the BM-SC that organizes the multicast mechanism, ought to keep an additional list with the multicast groups (Multicast group id) and the correspondent UEs that have joined them. This information is kept in the Multicast Groups List (Fig.4b) and the BM-SC has the opportunity to retrieve the UEs belonging to a

specific multicast group. It is essential that these lists are fully updated at every moment for the correct transmission of the packets to the UEs that have joined a multicast group. Obviously, there is a possibility that a multicast group has no members, which in turn means that the correspondent record in the Multicast Group List in the BM-SC does not contain any UEs.

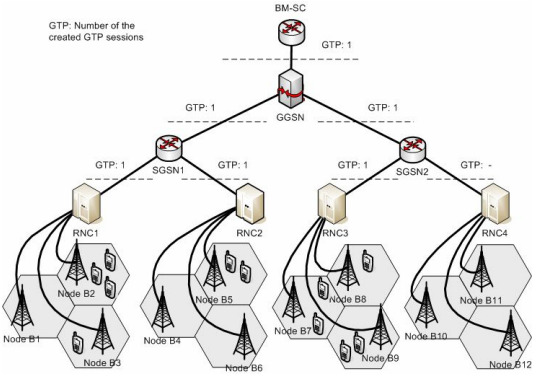


Fig. 3. Packet delivery in UMTS

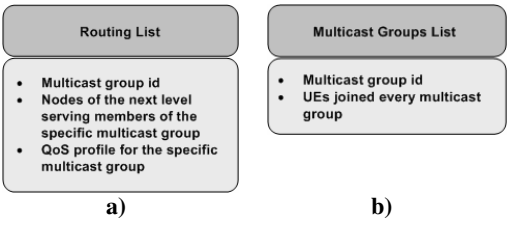


Fig. 4. Routing List and Multicast Groups List

Additionally, the phases that the multicast mechanism follows are these that have been presented above in the MBMS service provision (Fig. 2). In the following, we briefly describe the main steps of the multicast packet forwarding mechanism. Firstly, we consider that the UEs are known to the network, thus the Subscription phase is completed. In the Service Announcement phase, the routing lists of the nodes are filled with the useful information. This procedure can be initialized either from the UEs or from the BM-SC (i.e. Software upgrades). In the former case, consider a UE that decides to become a member of a multicast service. Thus, it sends an appropriate message to the BM-SC requesting this service. Then, every node located in the path between this UE and the BM-SC, when it receives the message from the UE, it updates its routing list and forwards the message to the next node. In the second case, the BM-SC initializes the Service Announcement phase. Since the BM-SC does not have any information regarding the location of the multicast members, a paging procedure at RA and URA level is necessary for the updating of the routing lists of the

nodes. The phases that follow are Session Start, MBMS Notification, Data Transfer and Session Stop, where the data are transferred from the BM-SC to the UEs. In these phases, each node of the network that receives a multicast packet, searches its routing list and decides the nodes of the next level that the packet should be forwarded. Finally, the packet reaches the UEs that are members of the multicast group.

With multicast, the packets are forwarded to those Node Bs that have multicast users. Therefore, in Fig. 3, the Nodes B2, B3, B5, B7, B8, B9 will receive the multicast packets issued by the BM-SC. We briefly summarize the five steps occurred for the delivery of the multicast packets. Firstly, the BM-SC receives a multicast packet and forwards it to the GGSN that has registered to receive the multicast traffic. Then, the GGSN receives the multicast packet and by querying its routing list, it determines which SGSCs in its service area have multicast users residing in their respective service areas. In Fig. 3, the GGSN duplicates the packet and forwards it to the SGSN1 and the SGSN2.

After both destination SGSNs have received the multicast packet and having queried their routing list, they determine which RNCs must receive the multicast packet. The destination RNCs receive the multicast packet and send it to the Node Bs that have established the appropriate radio bearers for the multicast application. In Fig. 3, these are Node B2, B3, B5, B7, B8, and B9. The multicast users receive the multicast packet on the appropriate radio bearers, either by point-to-point channels transmitted to individual users separately or by point-to-multipoint channels transmitted to all group members in the cell.

In this approach, each multicast packet is initially transmitted from the BM-SC to the GGSN. This procedure implies that the first GTP session is created between the BM-SC and the GGSN. The GGSN forwards exactly one copy of the multicast packet to each SGSN that serves multicast users. This leads to the creation of one GTP session between the GGSN and the SGSN1 and one GTP session between the GGSN and SGSN2 (Fig. 3). Having received the multicast packets, the SGSN1 forwards exactly one copy of the multicast packet to the RNCs that serve multicast users, which are the RNC1 and the RNC2. In parallel, the SGSN2 forwards the multicast packets to the RNC3, which is the only RNC, covered by the SGSN2 that serves multicast users. Regarding the edges between the SGSNs and the RNCs in Fig. 3, the first GTP session is created between the SGSN1 and RNC1, the second between the SGSN1 and RNC2 and the third one between the SGSN2 and RNC3. Finally, the RNCs forward the multicast packets to those Node Bs that multicast users reside in and have established the appropriate radio bearers. Additionally, Fig. 3 shows the exact number of the GTP sessions created in edges of the network for the multicast scheme.

The analysis presented in the above paragraphs, covers the forwarding of the data packets between the BM-SC and the Node Bs (Fig. 3). Therefore, the transmission of the packets over Uu and Iub interfaces may be performed on dedicated (Dedicated Channel - DCH) or common transport channels (FACH). DCH is a point-to-point channel and hence, it suffers from the inefficiencies of requiring multiple DCH to carry common data to a group of users. However, DCH can employ fast closed-loop power control and soft handover mechanisms to achieve a highly reliable channel. As presented in [12], point-to-multipoint MBMS data transmission uses the forward access channel (FACH) with turbo coding and QPSK modulation at a constant transmission power. Multiple services can be configured in a cell, either time multiplexed

on one FACH or transmitted on separate channels, although in the latter case a single UE may not be able to receive multiple services. Control information, for example, available services, neighboring cell information indicating which of the neighboring cells that transmit the same content and so forth, is transmitted on a separate FACH.

4 Evaluation of the Multicast Scheme

In this section we present an evaluation, in terms of the telecommunication costs, of the multicast scheme presented in the previous section. We consider a more general UMTS network topology and different transport channels for the transmission of the multicast data.

In particular, we consider a subset of a UMTS network consisting of a single GGSN and N_{SGSN} SGSN nodes connected to the GGSN. Furthermore, each SGSN manages a number of N_{ra} RAs. Each RA consists of a number of N_{rnc} RNC nodes, while each RNC node manages a number of N_{ura} URAs. Finally, each URA consists of $N_{node\text{b}}$ cells. The total number of RNCs and cells are:

$$N_{RNC} = N_{SGSN} \cdot N_{ra} \cdot N_{rnc} \tag{1}$$

$$N_{NODEB} = N_{SGSN} \cdot N_{ra} \cdot N_{rnc} \cdot N_{ura} \cdot N_{nodeb} \tag{2}$$

The total transmission cost for packet deliveries is considered as the performance metric. We make a further distinction between processing costs at nodes and transmission costs on links. Similar to [6] and [2], we assume that there is a cost associated with each link and each node of the network for the packet deliveries. We apply the following notations:

D_{gs}	Transmission cost of packet delivery between GGSN and SGSG
D_{sr}	Transmission cost of packet delivery between SGSN and RNC
D_{rb}	Transmission cost of packet delivery between RNC and Node B
D_{DCH}	Transmission cost of packet delivery over the air with DCHs
D_{FACH}	Transmission cost of packet delivery over the air with FACH
p_g	Processing cost of packet delivery at GGSN
p_s	Processing cost of packet delivery at SGSN
p_r	Processing cost of packet delivery at RNC
p_b	Processing cost of packet delivery at Node B

The total number of the multicast UEs in the network is denoted by N_{UE}. For the cost analysis, we define the total packets per multicast session as N_p. Furthermore, network operators will typically deploy an IP backbone network between the GGSN, SGSN and RNC. Therefore, the links between these nodes will consist of more than one hop. Additionally, the distance between the RNC and Node B consists of a single hop ($l_{rb} = 1$). In the presented analysis we assume that the distance between GGSN and SGSN is l_{gs} hops, while the distance between the SGSN and RNC is l_{sr} hops.

In multicast, the SGSNs forward a single copy of each multicast packet to those RNCs serve multicast users. After the correct multicast packet reception at the RNCs the RNCs forward the multicast packets to those Node Bs that have established the appropriate radio bearers via Dedicated or Common Transport Channels. The total

cost for the multicast scheme is derived from the following equation where n_{SGSN}, n_{RNC}, n_{NODEB} represent the number of SGSNs, RNCs, Node Bs respectively, that serve multicast users.

$$M_S = \left[p_g + n_{SGSN} \left(D_{gs} + p_s \right) + n_{RNC} \left(D_{sr} + p_r \right) + n_{NODEB} \cdot p_b + X \right] N_p \tag{3}$$

$$X = \begin{cases} n_{NODEB} \cdot N_{UE} \cdot D_{rb} + D_{DCH} \cdot N_{UE}, if \quad channel = DCH \\ n_{NODEB} \cdot D_{rb} + D_{FACH} \cdot n_{NODEB}, if \quad channel = FACH \end{cases} \tag{4}$$

The parameter X represents the multicast cost for the transmission of the multicast data over the Iub and Uu interfaces. This cost of the multicast scheme depends mainly on the distribution of the multicast group within the UMTS network and secondly on the transport channel that is used. In cells that the multicast users' density is high, the use of common channels such as FACH is preferable to the use of a DCH since the latter is reserved only for a single user.

An issue that should be noticed regarding the eqn(4) is that the first term in each of the two legs of the eqn(4) represents the packet delivery cost over the Iub interface which depends on the radio bearer used for the transmission of the data over the Iub. In case we use the FACH as transport channel each multicast packet send once over the Iub interface and then the packet is transmitted to the UEs that served by the corresponding Node B. However, in case we use DCHs for the transmission of the multicast packets over the Iub each packet is replicated over the Iub as many times as the number of multicast users that the corresponding Node B serves.

5 Results

Having analyzed the costs of the multicast scheme, we try to evaluate the cost in function of a number of parameters. The first parameter is the number of the total packets per multicast session (N_p) and the second one is the number of the multicast users (N_{UE}). We assume a more general network configuration than that illustrated in Fig. 3, with N_{SGSN} =10, N_{ra} =10, N_{rnc} =5, N_{ura} =5 and N_{nodeb} =5. As we can observe from the equations in the previous section, the cost of the scheme depends on a number of other parameters. Thus, we have to estimate the value of these parameters appropriately, taking into consideration the relations between them. The chosen values of the parameters are presented in Table 1.

Table 1. Chosen parameters' values

D_{gs}	D_{sr}	D_{rb}	p_g	p_s	p_r	p_b	D_{DCH}	D_{FACH}	l_{gs}	l_{sr}	l_{rb}
36	18	6	1	1	1	1	3	5	6	3	1

The packet transmission cost (D_{xx}) in any segment of the UMTS network is proportional to the number hops between the edge nodes of this network segment. This means that $D_{gs} = \lambda\, l_{gs}$,$D_{sr} = \lambda\, l_{sr}$ and $D_{rb} = \lambda\, l_{rb}$. For the cost analysis and without loss of generality, we assume that the distance between the GGSN and SGSN is 6 hops (l_{gs} = 6), while the distance between SGSN and RNC is 3 hops (l_{sr} = 3).

In our analysis, the values for the transmission costs of the packet delivery over the air with each of the two transport channels are different. More specifically, the transmission cost over the air with Dedicated Channels (D_{DCH}=3), is smaller than the cost of the packet delivery over the air with FACH (D_{FACH}=5). The main difference between the Dedicated and Common resources is that FACH does not allow the use of fast power control. In particular, as presented in [13] the MBMS service can take significant portion of the sector power if FACH is used to carry the MBMS traffic. As a Common Channel (FACH) needs to be received by all the UEs in the cell, also those near the cell's border, it requires more radio resources (power) than a DCH.

In order to calculate the number of the UMTS nodes that serve multicast users, we define the following probabilities:

P_{SGSN}: The probability that an SGSN serve multicast users

P_{RNC}: The probability that an RNC (served by an SGSN with multicast users), serves multicast users

P_{NODEB}: The probability that a Nobe B (served by an RNC with multicast users), serves multicast users

For the cost analysis, we assume that P_{SGSN}=0.4, P_{RNC}=0.3 and P_{NODEB}=0.4. Consequently, the number of the SGSNs, the RNCs and the Node Bs that serve multicast users is derived from the following equations:

$$n_{SGSN} = N_{SGSN} \cdot P_{SGSN} = 4 \tag{5}$$

$$n_{RNC} = N_{RNC} \cdot P_{SGSN} \cdot P_{RNC} = 60 \tag{6}$$

$$n_{NODEB} = N_{NOBEB} \cdot P_{SGSN} \cdot P_{RNC} \cdot P_{NODEB} = 600 \tag{7}$$

Fig. 5 presents the cost of the multicast scheme in function of the N_p for different transport channels (DCH and FACH) used for the transmission of the multicast data over the air. The y-axis presents the total cost of the multicast scheme, while the x-axis shows the total packets per multicast session.

Regarding the use of DCHs, in Fig. 5, we have calculated the costs for three different values of the number of multicast users. Fig. 5 indicates that the multicast cost increases rapidly when the amount of the multicast data increases. Furthermore, for a given N_p, the multicast cost increases as the members of the multicast group increase. This is because the greater the number of multicast users is, the greater the number of DCHs needed for the transmission of the multicast data over the air and finally the greater the multicast cost is according to eqn (3) and eqn (4). Additionally, eqn (3) shows that in case we use FACH for the transmission of the multicast data over the air, the cost of the multicast scheme depends only on the number of packets per multicast session and not on the number of multicast users. This can be shown in Fig. 5 where we can observe that the greater the N_p is, the greater the multicast cost becomes.

Another interesting observation that comes out from Fig.5 is that for small numbers of multicast users the use of DCHs is preferable to the FACHs. One of the key assumptions in MBMS is that if the number of UEs within a cell using a particular

MBMS service is high enough, it will be advantageous to broadcast the MBMS data stream over the whole cell. If the number of UEs is low, serving each UE through DCHs means might be more efficient. A reasonable threshold for switching from point to point radio bearers to point to multipoint radio bearers in the multicast case is the number of 7-15 active MBMS users per cell [14].

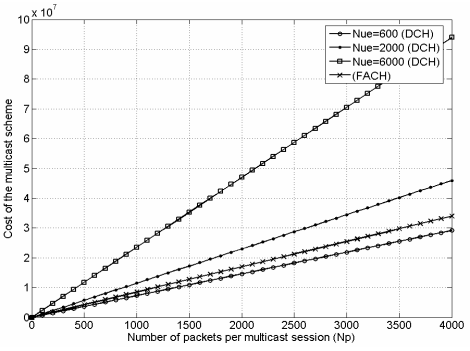


Fig. 5. Cost of the multicast scheme against *Np* for different transport channels

Furthermore, we try to estimate the cost of the multicast scheme in function of the N_{UE} (Fig. 6). As we observe, three different values of the number of the total packets per multicast session (N_p) have been calculated. Fig. 6a presents the cost of the multicast scheme against N_{UE} in case we use FACH for the transmission of the multicast data over the air. According to Fig. 6a, the cost of the multicast scheme is independent from the number of multicast users in case we use FACH for the transmission of the multicast data over the air. The cost of the multicast scheme in this case depends mainly on the number of Node Bs that serve multicast users. Only one FACH per cell is established and it is capable of supporting a great number of multicast users in this cell. Regarding the multicast cost against N_{UE} in case of the DCHs, the relation between them is predictable, since the greater the number of the multicast UEs is, the greater the cost becomes (Fig. 6b).

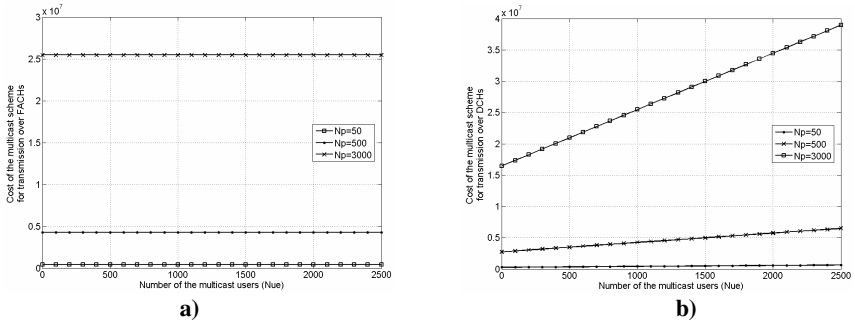


Fig. 6. Costs of the multicast scheme against N_{UE} using different transport channels

Fig. 7 indicates that with multicast, the total transmission cost if we use common channels such as FACH is lower than the cost if we use DCHs. More specifically, Fig. 7a presents the costs of the multicast scheme in function of the N_p (for N_{UE}=2000) using different transport channels, while Fig. 7b presents the costs of the multicast scheme in function of the N_{UE} (for N_p=3000) using different transport channels.

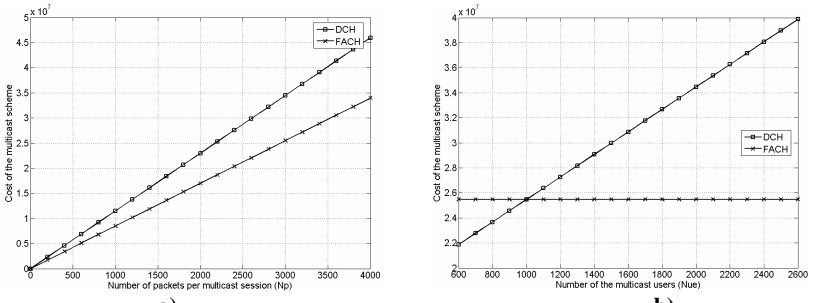


Fig. 7. Costs of the multicast scheme against N_p and N_{UE} using different transport channels

Another interesting parameter is the P_{NODEB}, which is the probability that a Node B, served by an RNC with multicast users, serves multicast users. Obviously, this probability takes values from 0 to 1. In case that P_{NODEB} converges to zero, the multicast users are located to a limited number of cells. On the other hand, when the P_{NODEB} converges to the value 1, then the multicast users are spread to many cells. Assuming that N_{UE}=1500, N_p=500, we can calculate the cost for the multicast scheme from the eqn(3) and eqn(4).

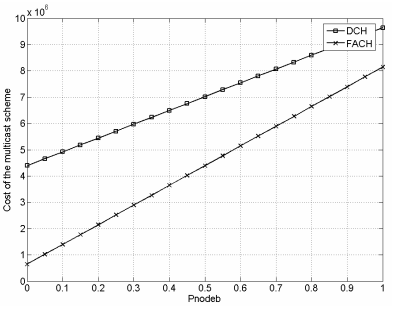


Fig. 8. Cost of the multicast scheme against P_{NODEB} for different transport channels

Fig. 8 presents the cost of the multicast scheme in function of P_{NODEB} for different transport channels. It is obvious from Fig. 8 that the cost of the multicast scheme is decreased as P_{NODEB} converges to zero. This means that the greater the number of multicast users per cell is, the lower the cost of the multicast scheme is. Furthermore, regarding the use of different transport channels for the transmission of the multicast data through the air, the use of FACHs is absolutely preferable to the use of DCHs as Fig. 8 indicates.

6 Conclusions and Future Work

In this paper, we have presented a multicast scheme for UMTS and the delivery of the multicast packets to a group of mobile users and have analyzed the performance of such a delivery in terms of the telecommunication cost. Considering a general network configuration, we have analyzed the cost of a multicast scheme in function of a number of parameters. Such parameters are the number of multicast users within the multicast group, the amount of data sent to the multicast users and finally the density of the multicast users within the cells. Additionally, we have evaluated the performance of the multicast scheme considering different transport channels for the transmission of the multicast data over the air. The step that follows this work is to carry out experiments using the NS-2 simulator.

References

1. Hauge, M., Kure, O.: Multicast in 3G networks: Employment of existing IP multicast protocols in UMTS. in Proc. WoWMoM 2002, (2002) 96–103
2. Rummler, R., Chung, Y., Aghvami, H.: Modeling and Analysis of an Efficient Multicast Mechanism for UMTS. IEEE Trans. Vehicular Technology, vol. 54, no. 1 (2005) 350-365
3. Lin, Y.: A multicast mechanism for mobile networks. IEEE Communication Letters, vol. 5 (2001) 450–452
4. Rummler, R., Aghvami, H.: End-to-end IP multicast for software upgrades of reconfigurable user terminals within IMT-2000/UMTS networks. in Proc. IEEE ICC'02, vol. 1 (2002) 502–506
5. 3GPP TS 23.246 V6.9.0, Technical Specification Group Services and System Aspects; MBMS; Architecture and functional description (Release 6) (2005)
6. Ho, J. S., Akyildiz, I. F.: Local anchor scheme for reducing signaling costs in personal communications networks. IEEE/ACM Transactions on Networking, vol. 4 (1996) 709–725
7. Yang, S. R., Lin, Y. B.: Performance evaluation of location management in UMTS. IEEE Transactions on Vehicular Technology, vol. 52, no. 6 (2003) 1603-1615
8. 3GPP TS 23.060 V7.0.0, Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2 (Release 7) (2006)
9. Holma, H., Toskala, A.: WCDMA for UMTS: Radio Access for Third Generation Mobile Communications. John Wiley & Sons (2003)
10. Gossain, H., Cordeiro, C. Argawal, D.: Multicast: Wired to Wireless. IEEE Communications Magazine (2002) 116-123
11. Dutta, A., Chennikara, J., Chen, W., Altintas, O., Schulzrinne, H.: Multicast Media to Mobile Users. IEEE Communications Magazine (2003) 81-88
12. 3GPP TS 22.146 V7.1.0, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service; Stage 1 (Release 7) (2006)
13. Alexiou, A., Antonellis, D., Bouras, C.: A Multicast Approach for UMTS: A Performance Study. in Proc. IFIP Networking 2006, (2006) 1086 – 1091
14. Boni, A., Launay, E., Mienville, T., Stuckmann, P.: Multimedia Broadcast Multicast Service – Technology Overview and Service Aspects, In Proc of Fifth IEE International Conference on 3G Mobile Communication Technologies, (2004), 634-638

Scheme for Improving Transmission Performance of Realtime Traffic in Handover Between HMIPv6 Intermap Domains

Wongil Park, Jonghyoun Choi, and Byunggi Kim*

Department of Computer Science, Soongsil University
prudent_woman@yahoo.co.kr, wide@sunny.ssu.ac.kr,
bgkim@computing.ssu.ac.kr

Abstract. Many studies have been performed to improve the efficiency of mobile IP. Hierarchical MIPv6 (HMIPv6) was proposed due to the lack of MIPv6. The new protocol, that is, Mobility Anchor Point (MAP) receives all packets in place of Mobile Node (MN) and MAP services are transferred to Care of Address (CoA) of MN. However, it can affect the whole network owing to concentration phase of registration occurred in hierarchical MAP structure. We propose the scheme that selects different MAP according to the traffic characteristic. The quantitative result and performance analysis presented in this paper show that our proposal can reduce the cost of location update by 5% and total cost of MN that moves frequently by 34%.

1 Introduction

It is difficult for Mobile IPv6 (MIPv6) to support nodes with high mobility, because it is designed for low mobility devices [1, 5]. Adding a new service area, a MN acquires a new address and informs the home agent (HA) of this new address through binding update message. The HA is located on its home network which might be far away from the current location. That is the reason why the connection setup delay and packet loss occur. Thus it influences end-to-end QoS of real-time traffic [1, 2].

Hierarchical MIPv6 (HMIPv6) was proposed to solve this problem. MAP is introduced to improve the binding problem of MIPv6 [3]. It acts as a temporary HA in the network.

In Fig. 1, we assume that a MN is associated with AR1. MAP will play a role of temporary HA. AR1 will be the local access router. The MN receives system information both from the MAP and from the local router. The MN generates a Regional Care of Address (RCoA) and an on-Link Care of Address (LCoA). The MN registers itself on the system using RCoA and LCoA. When lots of MNs are allocated to a single MAP in a hierarchical Mobile IP network, it might incur significant

* This work was supported by the Korea Research Foundation Grant (KRF-2004-005-D00198).

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 25 – 36, 2006.

signaling overhead and processing overload [4, 7]. To avoid these problems, MNs should be evenly distributed to all MAPs.

This paper proposes a load balancing scheme for a MAP in a hierarchical Mobile IP network. The structure of this paper is as follows. In section 2, we describe the mobility of MN in HMIPv6. Next, in section 3, we explains traffic characteristic of MN of MAP selection scheme proposed in this paper. In section 4, we describe the performance evaluation by numerical analysis. Finally, section 5 offers conclusion.

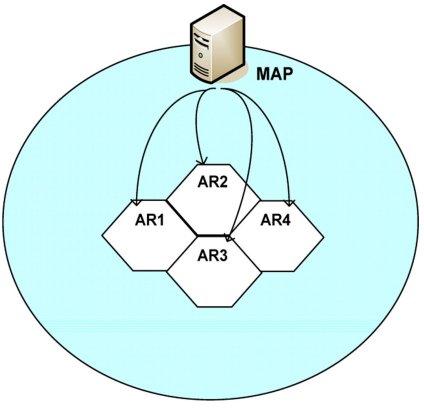


Fig. 1. HMIPv6 network structure

2 Related Works

There are several issues relating MAPs in a hierarchical Mobile IP. The first issue is which Access Router (AR)s would take roles of MAPs in a hierarchical network configuration. There are two options: one is to allow any AR in a hierarchical network to be a MAP and the other is to allow only a subset of ARs to be MAPs.

The second issue is on the load management of MAPs. It depends on the MAP configuration and the number of MNs. MAPs themselves which are responsible for mobility control of mobile terminals can be hierarchically configured. A decision algorithm is required on which MAP takes charge of each terminals. It is the problem of hierarchical configuration of MAPs and the access mechanism to them.

The third issue is how to relate mobility characteristic of MN to MAP selection.

For efficient mobility management of MNs, MAPs are introduced in HMIPv6. They act as local HAs. MAPs make it possible to provide better performance while minimizing modification of MIPv6 [6].

There are two kinds of handovers in HMIPv6 as shown in Fig. 2: micro handover and macro handover. In Fig. 2 micro handover occurs when a MN in the service area of AR1 of MAP2 enters the service area of AR3 of MAP2. Both AR1 and AR3 are under control of the same MAP2. Therefore the MN's MAP is not changed.

When a MN moves from the service area of AR3 of MAP2 to that of AR1 of MAP3, a macro handover occurs. Its MAP is changed from MAP2 to MAP3. In case of micro handover, LCoA is changed but RCoA is not. So it needs to send a Binding Update (BU) message neither to the original HA nor to the Correspondent node (CN). The MN still sends IP packets to MAP of CN and MAP forwards it to the correspondent.

However, macro handover accompanies MAP change. Therefore the BU message, which includes the new RCoA, must be sent to the original HA and the CN. It will increase handover delay. In this way MN's mobility has influence on handover performance and eventually on the configuration and selection of MAPs.

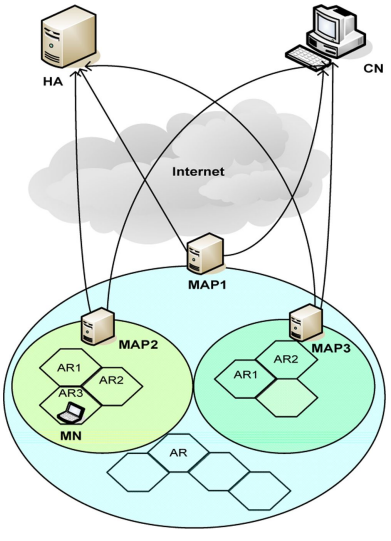


Fig. 2. The basic operation of the HMIPv6

3 MAP Selection Based on the Traffic Characteristic

3.1 MAP Selection by Traffic Characteristic of MN

A MN selects generally a MAP using the MAP option in Router Advertisement (RA) message received from MAP or AR. We propose a new scheme that Next MAPs (NMAPs) are predicted to reduce handover delay. The class of communication service is used as selection criteria for NMAP. The class of communication service is important to select the MAP. So, we consider the communication service that is used by MN. If MN uses realtime service, a rapid processing method should be prepared for realtime traffic processing during handover. Therefore, we should be consider what is the service using MN now. Also, we must choose MAP that can process

rapidly the handover if handover is occurred. The traffic characteristics of MN are divided into realtime traffic such as multimedia traffic or voice traffic and data traffic such as best effort traffic. The characteristics of traffic are closely related to QoS of MN and also it should be an important element to choose MAP. It is shown as Table 1.

Table 1. Traffic characteristic of MN

traffic characteristic	type
realtime traffic	streaming data traffic such as video or voice data traffic
Non-realtime traffic	data traffic such as best effort traffic

Handover delay is more affected by handover between MAPs than handover between ARs because realtime traffic is susceptible to handover delay. When MN moves to another area, MN sends BU (Binding Update) message. BU requires approximately 1.5 round trip times between the MN and each CN. In addition, one round-trip time is needed to update the HA; this can be done simultaneously while updating CNs. These round trip delays will disrupt active connections whenever a handoff to a new AR is performed. Moreover, in the case of wireless links, such a solution reduces the number of messages that sent to all CNs and the HA over the air interface. Accordingly, MAP selection by the distance is very important.

In Fig. 3, shows proposed system model.

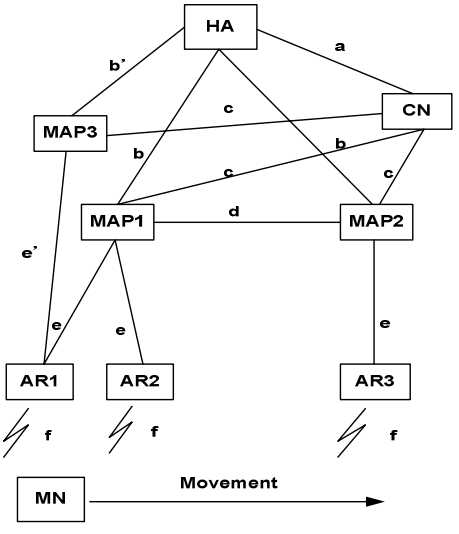


Fig. 3. System model of the proposed scheme

In this paper, we propose a MAP selection scheme based on the traffic characteristic. If mobility frequency of MN is high, the speed of MN is very fast. However, if mobility frequency of MN is low, the speed of MN is slow relatively. As a result, if MN moves into one cell and cell resident time is short, then we may guess that MN moves very fast. If cell resident time is long, MN moves slow.

4 Performance Evaluations

4.1 Mobility Model

We assumed that there is hexagonal cellular network architecture, as shown in Fig. 4. Each MAP domain is assumed to consist of the different number of range rings, D. Rings of cells surround each cell as shown in Fig.4 [8]. Each ring d (d>=0) is composed of 6d cells. The innermost cell "0" is called the center cell. The cells labeled by 1 form the first ring around cell "0", the cells labeled by 2 form the second ring around cell 0 and so forth. The number of cells N (D) is calculated using the following equation:

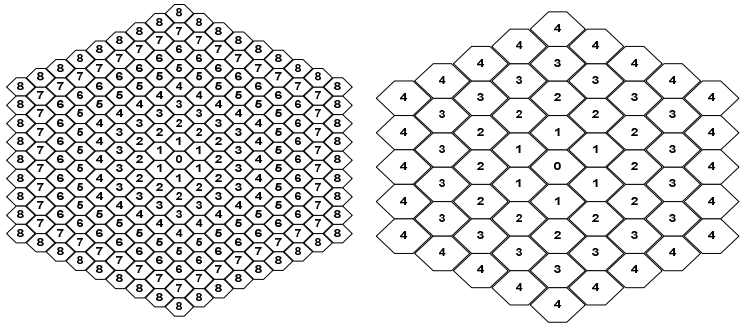


Fig. 4. Left is Hexagonal Cellular Network Architecture (d=8) and Right is Hexagonal Cellular Network Architecture (d=4)

$$N(D) = 1 + 6 \cdot \sum_{d=1}^{D} d = 1 + 3 \cdot D \cdot (D + 1) \quad (1)$$

Hexagonal Cellular Network Architecture (d=8) of Figure 4 shows the proposed hexagonal cellular network architecture of traffic characteristics.

The random-walk model is appropriate for pedestrian movements where mobility is generally confined to a limited geographical area such as residential and business buildings in the respect of user mobility model [9].

We consider the two-dimensional model used in Markov chain model in the respect of user mobility model [9]. In this model, the next position of an MN is equal to the previous position plus a random variable whose value is drawn independently from an arbitrary distribution. In addition, an MN moves to another cell area with a

probability of 1-q and remains in the current cell with probability, q. If an MN is located in a cell of ring d (d>0), the probability that a movement will result in an increase (p+(d)) or decrease(p-(d)) in distance from the center cell is given by

$$P^{+}(d) = \frac{2d+1}{6d} \quad and \quad P^{-}(d) = \frac{2d-1}{6d} \tag{2}$$

We define the state k of a Markov chain as the distance between the current cell of the MN and the center cell. This state is equivalent to the index of a ring in which the MN is located. As a result, the MN is said to be in state k if it is currently residing in ring d. The transition probabilities $\alpha_{d,d+1}$ and $\beta_{d,d-1}$ represent the probabilities of the distance of the MN from the center cell increasing or decreasing, respectively. They are given as follow:

$$\alpha_{d,d+1} = \begin{cases} (1-q) & if \quad d = 0 \\ (1-q)\,p^{+}(d) & if \quad 1 \le d \le D \end{cases} \tag{3}$$

$$\beta_{d,d-1} = (1\text{-}q)\ p^{-}(d) \qquad if \quad 1 \le d \le D \tag{4}$$

where q is the probability that an MN stays in the current cell.

We denote $p_{d,D}$ as the steady-state probability of state d within a MAP domain consisting of D range rings. As Eq.(3) and Eq.(4), $P_{d,D}$ can be expressed in terms of the steady state probability $P_{0,D}$ as follows:

$$P_{d,D} = P_{0,d} \prod_{i=0}^{d-1} \frac{\alpha_{i,i+1}}{\beta_{i+1,i}} \qquad \text{for } 1 \le d \le D \tag{5}$$

With the requirement $\sum_{d=0}^{D} P_{d,D} = 1$, $P_{d,D}$ can be expressed by

$$P_{0,D} = \frac{1}{1 + \sum_{d=1}^{D} \prod_{i=0}^{d-1} \frac{\alpha_{i,i+1}}{\beta_{i+1,i}}} \tag{6}$$

where $\alpha_{d,d+1}$ and $\beta_{d,d-1}$ are obtained from Eq.(3) and Eq.(4)

4.2 Cost Functions

In order to analyze the performance of wireless/mobile networks, the total cost, consisting of location update cost and paging cost, should be considered. However, since HMIPv6 [3] does not support paging functions, we divide the total cost into location update cost and packet delivery cost. In proposed scheme, we divide total cost into new location update and packet delivery cost. The location update cost, new location update and the packet delivery cost are denoted by $C_{location}$, $C_{new\text{-}location}$, and C_{packet}, respectively. Then, the total cost of HMIPv6 (C_{total}) and proposed scheme ($C_{new\text{-}total}$) can be obtained as follows:

$$C_{total} = C_{location} + C_{packet} \tag{7}$$

$$C_{new-total} = C_{new-location} + C_{packet} \tag{8}$$

4.2.1 Location Update Cost

When a MN moves into a new MAP domain, it needs to configure two CoAs: an RCoA on the MAP's link and an on-link CoA(LCoA). In HMIPv6, an MN performs two types of binding update procedures: the global binding update and the local binding update. In global binding update, an MN registers its RCoA with the CNs and the HA. On the other hand, if an MN changes its current address within a local MAP domain, it only needs to register to this registration. C_g , $C_{new\text{-}g}$ and C_l denote the signaling costs in the global binding update, the global binding update of proposed scheme and the local binding update, respectively. In the IP networks, the signaling cost is proportional to the distance between two network entities. C_g , $C_{new\text{-}g}$, and C_l can be obtained from the below equations.

$$C_g = 2 \cdot (k \cdot f + \tau \cdot (b + e)) + 2 \cdot N_{CN} \cdot (k \cdot f + \tau \cdot (b + c)) + PC_{HA} + N_{CN} \cdot PC_{CN} + PC_{MAP} \tag{9}$$

$$C_{new\_g} = 2 \cdot (k \cdot f + \tau \cdot (b'+e')) + 2 \cdot N_{CN} \cdot (k \cdot f + \tau \cdot (b'+c)) + PC_{HA} + N_{CN} \cdot PC_{CN} + PC_{MAP} \tag{10}$$

$$C_l = 2 \cdot (k \cdot f + \tau \cdot e') + PC_{MAP} \tag{11}$$

Here τ and k are the unit transmission costs in a wired and a wireless link, respectively. PC_{HA}, PC_{CN} and PC_{MAP} are the processing costs for binding update procedures at the HA, the CN and the MAP, respectively. Let b, b', c, e, e' and f be

the hop distance between nodes. N_{CN} denotes the number of CNs which are communicating with the MN.

HMIPv6 is an enhanced Mobile IPv6 to minimize the signaling cost using a local agent called MAP. The MAP can be located at any level in a hierarchical network of routers, including the AR. The MAP in HMIPv6 treats the mobility management inside a domain. Thus, when a MN moves around the sub-networks within a single domain, the MN sends a BU message only to the current MAP. In proposed scheme, we reduce the probability of the global binding update.

In terms of the random walk mobility model, the probability that a MN performs a global binding update is as follows:

$$P_{D,D} \cdot \alpha_{d,d+1} \tag{12}$$

Specifically, if a MN is located in range ring D, the boundary ring of a MAP domain is composed of D range rings, and performs a movement from range ring D to range ring D+1. The MN then performs the global binding update procedure. In other cases, except this movement, the MN only performs a local binding update procedure. Hence, the location update cost of normal and proposed scheme per unit time can be expressed as follows:

$$C_{location} = \frac{P_{D,D} \cdot \alpha_{D,D+1} \cdot C_g + (1 - P_{D,D} \cdot \alpha_{D,D+1}) \cdot C_l}{T} \tag{13}$$

$$C_{new-location} = \frac{P_{D,D} \cdot \alpha_{D,D+1} \cdot C_{new-g} + (1 - P_{D,D} \cdot \alpha_{D,D+1}) \cdot C_l}{T} \tag{14}$$

where T is the average cell residence time.

4.2.2 Packet Delivery Cost

The packet delivery cost, C_{packet}, in HMIPv6 can then be calculated as follows:

$$C_{PACKET} = C_{MAP} + C_{HA} + C_{CN-MN} \tag{15}$$

In Eq(15), C_{MAP} and C_{HA} denote the processing costs for packet delivery at the MAP and the HA, respectively. $C_{CN\text{-}MN}$ denotes the packet transmission cost from the CN to the MN.

In HMIPv6, a MAP maintains a mapping table for translation between RCoA and LCoA. The mapping table is similar to that of the HA, and it is used to track the current locations (LCoA) of the MNs. All packets directed to the MN will be received

by the MAP and tunneled to the MN's LCoA using the mapping table. Therefore, the lookup time required for the mapping table also needs to be considered. Specifically, when a packet arrives at the MAP, the MAP selects the current LCoA of the destination MN from the mapping table and the packet is then routed to the MN. Therefore, the processing cost at the MAP is divided into the lookup cost (C_{lookup}) and the routing cost ($C_{routing}$). The lookup cost is proportional to the size of the mapping table. The size of the mapping table is proportional to the number of MNs located in the coverage of a MAP domain [10]. On the other hand, the routing cost is proportional to the logarithm of the number of ARs belonging to a particular MAP domain [4]. Therefore, the processing cost at the MAP can be expressed as Eq. (17). In Eq.(17), λ_s denotes the session arrival rate and S denotes the average session size in the unit of packet.α and β are the weighting factors. Let N_{MN} be the total number of users located in a MAP domain. This paper assumes that the average number of users located in the coverage of an AR is K. Therefore, the total number of users can be obtained using Eq. (16).

$$N_{MN} = N_{AR} \times K \tag{16}$$

$$\begin{aligned} C_{MAP} &= \lambda_s \cdot \overline{S} \cdot (C_{lookup} + C_{routing}) \\ &= \lambda_s \cdot \overline{S} \cdot (\alpha N_{MN} + \beta \log(N_{AR})) \end{aligned} \tag{17}$$

In MIPv6, the route optimization is used to resolve the triangular routing problem. Therefore, the only first packet of a session transits the HA to detect whether an MN moves into foreign networks or not. Subsequently, all successive packets of the session are directly routed to the MN. The processing cost at the HA can be calculated as follows:

$$C_{HA} = \lambda_S \cdot \theta_{HA} \tag{18}$$

where Θ_{HA} refers to a unit packet processing cost at the HA.

Since HMIPv6 supports the route optimization, the transmission cost in HMIPv6 can be obtained using Eq. (19). As mentioned before, τ and κ denote the unit transmission costs in a wired and a wireless link, respectively.

$$C_{CN-MN} = \tau \cdot \lambda_s \cdot ((S-1) \cdot (c+e) + (a+b+e)) + k \cdot \lambda_s \cdot S \tag{19}$$

5 Numerical Results

In this section, we provide some numerical evaluation to demonstrate the performance of proposed scheme as compared with normal HMIPv6. The parameter values for the analysis were referenced from [10], [11] and [12]. They are shown in Table 2.

Table 2. Numerical simulation parameter for performance analysis

parameter	value	parameter	value	parameter	value
α	0.1	a	6	b'	3
β	0.2	b	6	e'	4
γ	0.05	c	4	N_{CN}	2
θ_{HA}	20	d	1	PC_{HA}	24
τ	1	e	2	PC_{MAP}	12
k	2	f	1	PC_{CN}	6

Fig 5 shows the variation in the location update cost as the average cell residence time is changed in the random-walk model. The location updates cost becomes less as the average cell residence time increases. In a comparison of proposed scheme with HMIPv6, proposed scheme reduces the location update cost by 5% approximately.

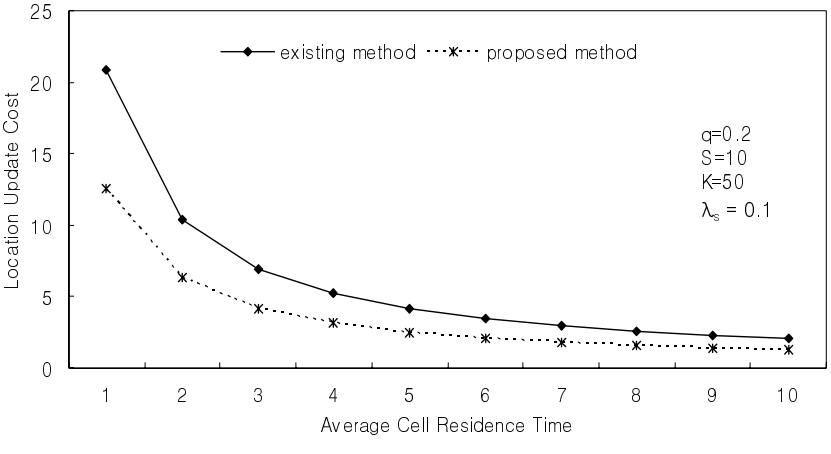


Fig. 5. Location update cost as function of average cell residence time of MN

Fig 6 shows the total cost of average cell residence time in random-walk model.

When the average cell residence time of MN is below 5 seconds, in the other words, MN moves frequently, MN is superior in respect of transmission ability of

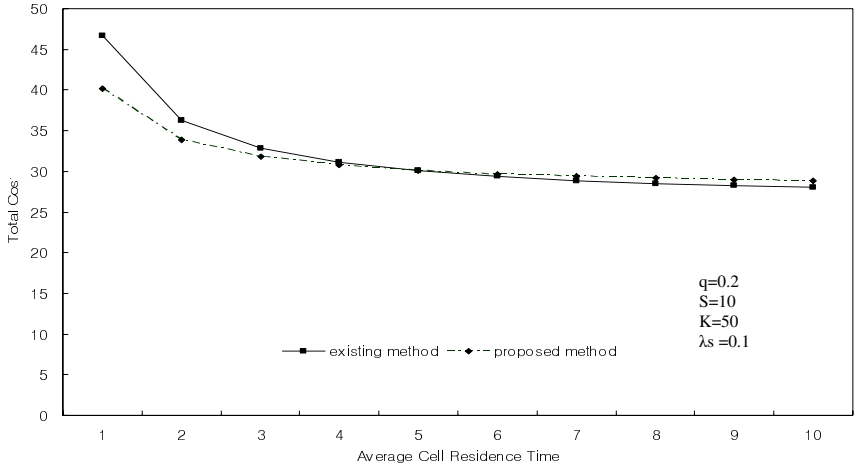


Fig. 6. Total cost as function of average cell residence time of MN

realtime traffic. As a result, if the cell residence time of MN is below 5 seconds, proposed method is preferred. However, if the cell residence time of MN is over 5 seconds, conventional method is preferred.

6 Conclusion

The MAP, which is proposed in HMIPv6, is proposed for mobility management of MNs. But, the connection requests are concentrated to the upper level MAPs. The concentration on specific MAP cannot guarantee the stable service for handover transaction according to overload and the failure on the selection of specific MAP leads to additional handover delay. Therefore, this paper proposed a scheme, which prevents concentration to the specific MAP by distributing connection requests to various MAPs based on the characteristic of mobile devices.

The proposed scheme reduces the location update cost by 5% and the total cost by 34% approximately.

References

1. D. Johnson, C. Perkins and J. Arrko, "Mobility support in IPv6," Internet Draft, IETF, draft-ietf-mobileip-ipv6-20.txt(work in progress), Jan. 2003.
2. J. Xie and F. Akyildiz, "A novel distributed dynamic location management scheme for minimizing signaling costs in Mobile IP," IEEE Trans. on Mobile Computing, Vol. 1, No, 3, pp. 163-175, Sep. 2002.
3. H. Soliman, C. Castelluccia, K. E. Malki and L. Bellier, "Hierarchical MIPv6 (HMIPv6) mobility management," Internet Draft, Nov. 2001.
4. Sangheon Pack, Byoungwook Lee, and Yanghee Choi, "Load Control Scheme at Local Mobility Agent in Mobile IPv6 Networks," WWC04, May. 2004.

5. S. Deering and B. Hinden, "Internet Protocol version6 (IPv6) specification," IETF, RFC2460, Dec. 1998.
6. P. Reinbold and O. Bonaventure, "A Comparison of IP Mobility Protocol," Tech. Rep. Infonet-TR-2001-07, University of Namur, Infonet Group, Jun. 2001.
7. Abbas Jamalipour, The Wireless Mobile Internet, Wiley, 2003.
8. J.S.M. Ho and I. F. Akyildiz, "Mobile user location update and paging under delay constrainsts," *ACM-Baltzer J. Wireless Networks*, vol. 1, pp. 413-425, Dec. 1995.
9. I.F. Akyildiz and W. Wang, "A dynamic location management scheme for next-generation multitier PCS systems," IEEE Trans. Wireless Commun., vol.1, no.1, pp.178-189, Jan. 2002.
10. Sangheon Pack and Yanghee Choi, " A Study on performance of hierarchical mobile IPv6 in IP-based cellular networks," IEICE Transactions on Communications, vol. E87-B no. 3 pp.462-469, Mar. 2004.
11. M. Woo, "Performance analysis of mobile IP regional registration," IEICE Trans. Commun., vol.E86-B, no.2, pp.472-478, Feb. 2003.
12. X. Zhang, J. G. Castellanos, and A. T. Capbell, "P-MIP: Paging extensions for mobile IP," ACM Mobile Networks and Applications, vol.7, no.2, pp.127-141, 2002.

DonorList: A New Distributed Channel Allocation Scheme for Cellular Networks

Tamer Tulgar and Muhammed Salamah

Eastern Mediterranean University, Department of Computer Engineering,
Famagusta,T.R.N.C
Mersin 10, Turkey
{tamer.tulgar, muhammed.salamah}@emu.edu.tr

Abstract. One of the most important challenges in cellular networks is to utilize the scarce spectrum allocated to the network in the most efficient way. If the channels are statically allocated to the cells, when a large number of mobile hosts move to the cell, that cell may run out of channels resulting in a high call incompletion rate. To overcome this problem, dynamic channel allocation schemes have been proposed. Among these schemes, distributed dynamic channel allocation approaches resulted in good performance results. Nevertheless, distributed allocation schemes must address the problem of efficient co-channel interference avoidance and reducing messaging overhead issues. In this paper, we introduced a new distributed channel allocation scheme namely the DonorList approach, which decreases the amount of messages required per channel allocation while efficiently handling the co-channel interference problem. We also demonstrate the performance results obtained after extensive simulation studies. The results show that the proposed algorithm outperforms the other algorithms recently proposed in the literature.

1 Introduction

In cellular wireless networks a mobile host(MH) can communicate with another MH anytime from anywhere with the help of base stations[1]. The area covered by the cellular network is divided into smaller regions called cells. Each cell is controlled by a base station and a MH communicates with its base station via a wireless link. All base stations in the cellular network can communicate with each other by using a wired network that connects every base station to the mobile switching center(MSC) of the cellular network[2].

A cellular system can use channels either as control channels, which carry control information like call setup data or as communication channels which carry the user data. In this paper, unless specified otherwise, the term *"channel"* will be referring to a *"communication channel"*.

When a call arrives at a cell, the base station should allocate a communication channel to support the incoming call. This process is known as the channel allocation process. If the base station fails to support the call, the call is said to be blocked or dropped. The most basic channel allocation scheme is known as

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 37–49, 2006.

the fixed channel allocation scheme (FCA), where each cell is preallocated with a fixed number of channels and the number of channels cannot vary depending on the system load [3]. In a FCA system, when a large number of mobile hosts move to the cell, that cell may run out of channels resulting in a high call incompletion rate. Since channels are very scarce resources, a channel allocation algorithm should not only assign a channel to a call but also must care about the channel usage efficiency by trying to increase the channel reuse [4]. For this purpose, dynamic channel allocation (DCA) schemes have been proposed [4],[5].

1.1 Dynamic Channel Allocation Schemes

In DCA schemes, unlike FCA, the number of channels allocated to each cell may vary depending on the needs of the cells. In a DCA scheme, a cell that has used all its nominal channels can borrow free channels from its neighboring cells(donors) to accommodate incoming calls. Additionally, the DCA schemes may be designed to rely on a pre-allocation of channels to the cells, which is also known as the *resource planning* or without any pre-allocation of channels to the cells. The DCA schemes can be classified as centralized dynamic channel allocation (C-DCA) schemes and distributed dynamic channel allocation (D-DCA) schemes.

In C-DCA schemes, only the MSC has access to the channel allocation information of the cells. In this approach, if a cell runs out of channels, the MSC is responsible for allocating new channels to the cell. In C-DCA schemes, the MSC is a single point of failure since it is the only unit which can assign channels to the cells and furthermore C-DCA schemes are not very scalable since the MSC can become a bottleneck under very heavy traffic conditions. To overcome these drawbacks, several D-DCA schemes have been proposed [6],[7],[8],[9],[10],[11],[12].

In a D-DCA scheme, there is no central controller like the MSC but instead every base station shares the responsibility to allocate channels (base stations import/export or borrow/lend channels to/from each other, depending on their *own local channel usage information* of the other cells). In the D-DCA schemes, if a cell needs to borrow/import a channel, it consults its neighbors by sending and receiving messages, and they negotiate together to ensure that no co-channel interference will occur when a channel(s) will be supplied to the cell in need.

In this paper, we propose a new D-DCA scheme based on resource planning. The main drawback of the previously proposed D-DCA algorithms is the high messaging overhead per channel allocation. The proposed algorithm employs a donor list, which is a list of import candidate channels and cells, to decrease the messaging complexity and to further improve the call completion probabilities compared to the D-DCA algorithms currently found in the literature. Also, the proposed algorithm is based on an import/export relation rather than a borrow/lend relation, where a cell gains the full control of the imported channels, and can export them to other cells.

The rest of this paper is organized as follows. In section 2, the system infrastructure is presented. In section 3, the proposed DonorList algorithm is explained in detail and in section 4 the performance evaluation and the simulation results of the algorithm are presented. Finally, in section 5, we present our conclusions.

2 System Model

The cellular system that is used to realize the *DonorList* algorithm contains 144 hexagonal cells, which are organized in a form of 12x12 grid. In the infrastructure of the employed cellular network, the 144 cells are partitioned into 7 reuse groups such that the cells in the same reuse group are apart from each other by at least a minimum distance defined by D_{min} in equation (1), where N is the cluster size which is the number of cells in a reuse group[2]. Each cell in the system, except the ones situated at the borders, has 6 neighbors.

$$D_{min} = \sqrt{3 \times N} \tag{1}$$

In Fig. 1, it can be seen that, the cells belonging to the same reuse group are labeled with a unique *Group ID* using the letters **{A,B,C,D,E,F,}**, and each cell is also labeled with a unique *Cell ID* using the integers ranging from **{1..144}**. The total channel spectrum belonging to the whole cellular system contains S = 280 channels [12]. Each channel is assigned a unique *Channel ID* ranging from 1 to 280. Initially each cell is assigned 40 channels by using the resource planning scheme explained in the next subsection.

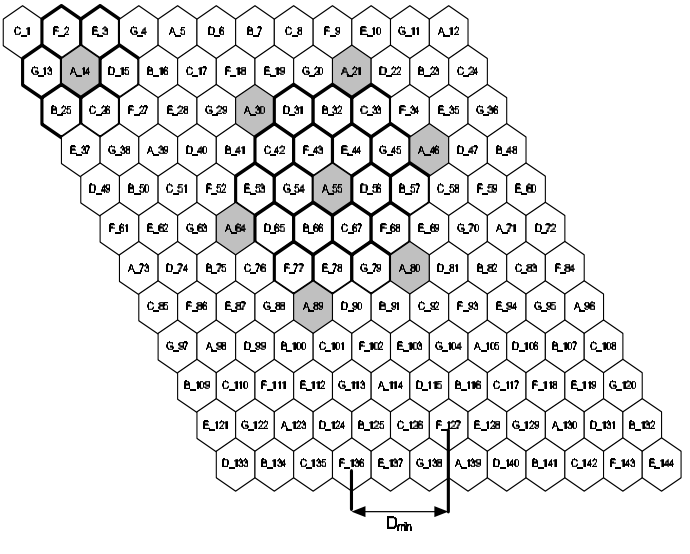


Fig. 1. Cellular System Layout

2.1 Resource Planning

Resource planning that will be used by the proposed DonorList algorithm is as follows:

- Partition the whole spectrum of channels(i.e. 280 channels) into 7 disjoint subsets and name them as P1..P7.
- Uniquely assign a channel group to each of the cell groups (A,B,C,D,E,F,G) such that the channels in P1 will only belong to the cells in group-A, channels in P2 will only belong to the cells in group-B and so on.
- Prioritize the channels in each cell in such a way that the smaller *Channel ID* will have a high priority and greater *Channel ID* will have a lower priority.
- The interference neighbors of a cell C_i, denoted as IN_i is defined as set of cells which have a distance smaller than the D_{min} from cell C_i. For example in Fig. 1, the IN_{55} set of the cell C_{55} contains the cells 31, 32, 33, 42, 43, 44, 45, 53, 54, 56, 57, 65, 66, 67, 68, 77, 78, 79.

$$IN_i = \{C_j | distance(C_i, C_j) < D_{min}\} \tag{2}$$

- A cell C_i can import channels only from its interference neighbors, provided that the same channel is not used within the interference distance of C_i.
- A base station assigns high priority channels to the incoming calls (i.e. new and handoff calls) and tries to export the lower priority channels for incoming channel import requests from other cells.

3 The Proposed DonorList Algorithm

In the cellular system described above, the proposed *DonorList* algorithm is executed separately by each cell. Each cell employs a channel usage threshold (C_t) which is used to warn a cell about its remaining number of *available* channels. Let us define the channel usage ratio of a cell C_i (CU_i) as the ratio of the number of busy channels of C_i to the number of the available channels of C_i, which is given in equation (3). When CU_i raises above C_t, C_i queries the cells in its IN_i, and collects information about which channels can be imported and forms a list called *the donor list*.

$$CU_i = \frac{number\_of\_busy\_channels\_of\_C_i}{number\_of\_total\_channels\_of\_C_i} \tag{3}$$

When the cell C_i runs out of available channels, it consults its donor list and asks for channel(s) starting from the cell(s) placed at the top of the list. If those cells can still export the channel to the cell C_i, they send their corresponding confirmations. If all these cells agree to export the channel to C_i, the exporter cells deallocate the exported channel to make sure that no co-channel interference will occur. If a suitable channel cannot be found at the first row of the donor list, the cell C_i moves to the next row in the list and repeats the process. If the cell C_i queries all the cells in the donor list and cannot find a channel to import, it drops the call.

By the addition of the *DonorList* idea, the cells which need to import a channel, send *request* messages only during the donor list formation, and then they only need to send messages to the cells listed in the donor list. In this way, the algorithm tries to reduce the total number of messages required per successful allocation.

The proposed algorithm is composed of five modules which are: The incoming call module, receive acquire message module, receive confirm message module, build donor list module and the intrahandoff module.

3.1 The Incoming Call Module

Fig. 2 below shows the flowchart for processing an incoming call. When a call arrives at C_i, if the cell contains at least one available channel, it allocates the channel to the call immediately. After a channel is allocated to a call, the cell checks if its CU_i ratio is higher than the threshold C_t. If CU_i is higher than the C_t, the cell sends request messages to all the cells in its IN_i and updates its donor list.

If no channels are available, then the cell checks if there is at least one entry in its donor list. If the donor list is not empty, the cell sends an *acquire* message with the format acquire(msgid,tocell,callid,fromcell,requestedchannelid,timestamp) to each cell which currently own the requested channel listed in the donor list entry and removes the entry from the donor list. Also, the cell inserts the call information to a list called the waiting calls list. However, if the donor list is empty, the cell blocks or drops the call.

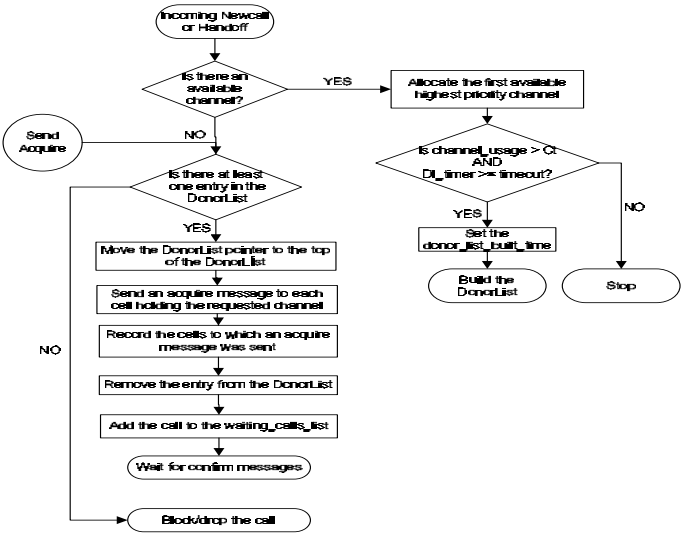


Fig. 2. Incoming Call Module

If the received signal signal strength(RSS) of a call drops below a predefined value RSS_{edge} , the RSS values received from the neighbor cells are calculated and the call is transferred to the control of the base station which provides the maximum RSS. This process is known as the handoff process. When a handoff occurs the handoff call is transferred to the new basestation as an incoming call and the new base station tries to allocate a channel to this incoming call.

3.2 Receive Acquire Message Module

When a cell receives an *acquire* message, it uses the algorithm given in Fig. 3 to process the message. So, when cell C_i receives an *acquire* message, first it checks if it has any waiting calls. If it has, the received *acquire* message is inserted into a queue, named as the acquire queue. If the waiting calls list of C_i is empty and the acquire queue is empty, then the *acquire* message is replied with a *confirm* "ok" message confirming that the requested channel is available or with a *confirm* "not ok" message informing the requesting cell that the requested channel is busy.

If there are queued *acquire* messages, the new *acquire* message is inserted into the acquire queue and all the messages in the queue are replied in the ascending order of their timestamps with corresponding *confirm* "ok" or *confirm* "not ok" messages. In any case, if the cell sends a *confirm* "ok" message, it immediately marks the requested channel as reserved.

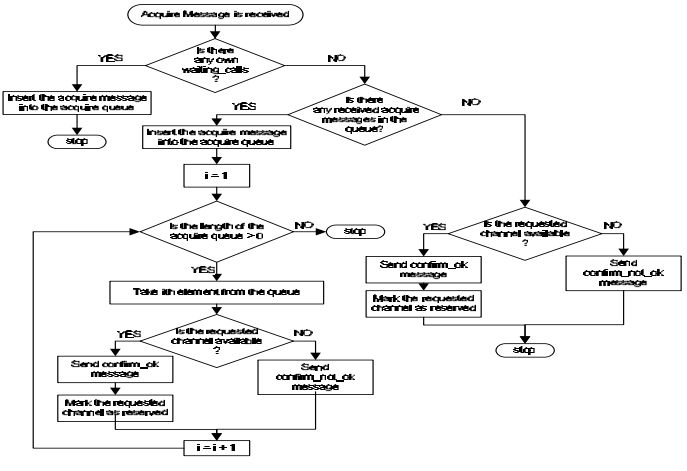


Fig. 3. Receive Acquire Module

3.3 Receive Confirm Message Module

The details of the processing of a received *confirm* message are shown in Fig. 4. If cell C_i receives *confirm* "ok" messages from all the cells which own the requested

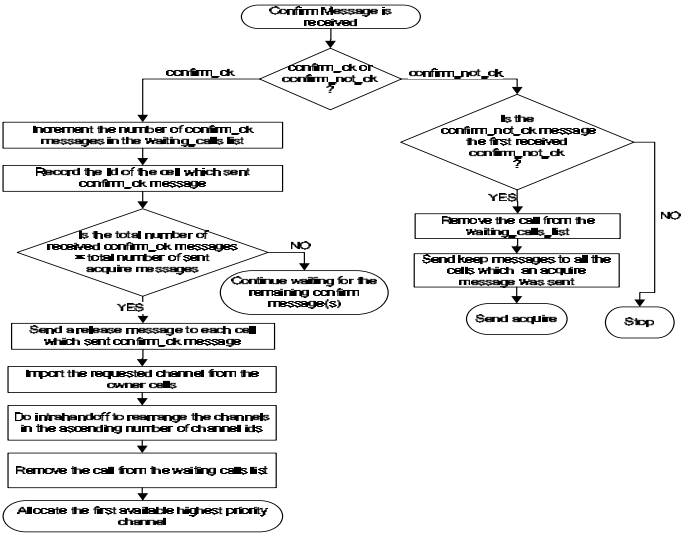


Fig. 4. Receive Confirm Module

channel, it imports the requested channel and sends a *release* message to each owner cell so that the cells which currently own the channel can remove the requested channel from their channel sets. Also, C_i removes the call from its waiting calls list.

If any of the owner cells send a *confirm* "not ok" message, the cell sends *keep* messages to the cell(s) which sent *confirm* "ok" messages, so that the channels they marked can be used again as available channels by their owners. Also, the cell deletes the call from the waiting calls list. Then, the cell runs its send acquire procedure which is shown in figure 2, so that the next entry in the donor list can be processed and new *acquire* messages can be send for another channel import attempt.

3.4 Intrahandoff Module

The intrahandoff module is triggered whenever a channel is deallocated at a cell(i.e. after an outgoing handoff, a terminated call or a successful channel import). This module moves the ongoing calls allocated at the low priority channels to the available high priority channels. In this way, the low priority channels are tried to be left available for possible import requests. This strategy raises the chance of finding at least one donorlist entry and so the successful import ratio of the algorithm.

3.5 Build Donor List Module

Fig. 5 illustrates the algorithm which builds a donor list. When a build donor list event is triggered, as explained in the incoming call module, a cell C_i sends

request(from cell, to cell) messages asking for the channel information of all the IN_i cells. On receiving request message, every cell send the set of its available(AC) and busy channels(BC) immediately. After all the reply(from cell, to cell, AC, BC) messages arrive at C_i, all the available channels are combined into a single AC set and all the busy channels are combined into a single BC set. Then, the candidate channels set are calculated by the set difference of AC and BC sets. The second set difference of the candidate channels set and the channels owned by C_i gives the real *candidates* set.

The calculated candidate channels set is then divided into subsets according to the common cells which own each channel. Each donor list entry is formed by selecting the channel with the maximum *Channel ID* and the cells which own the selected channel for each subset (i.e. an entry is formed for each subset). These entries is then inserted into the donor list in the order of descending number of channels in each subset. After insertion, the entries with the same number of channels are resorted in the order of ascending number of cells.

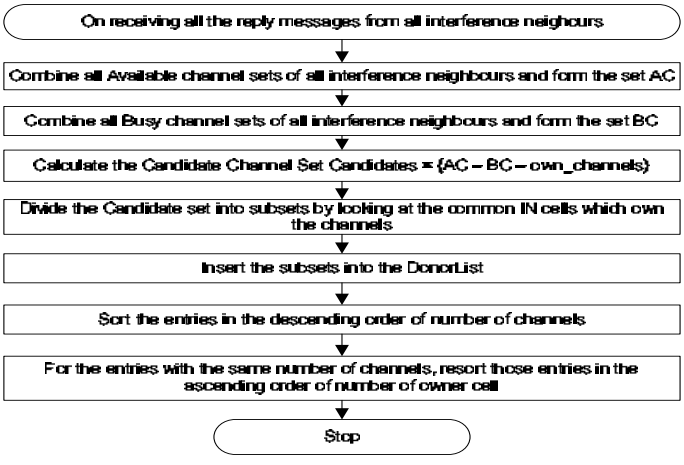


Fig. 5. Build Donor List Module

3.6 Deadlock Freedom of the Proposed DonorList Algorithm

In the proposed DonorList algorithm each message is timestamped using Lamport timestamps [13]. Also, it is assumed that the wired network connecting the basestations and the MSC is reliable and no messages will be lost and also the messages will be received at the cells in the order that they were sent. Based on these assumptions, request messages coming from different cells can be totally ordered by their timestamps [12].

Since the timestamps of the messages are known to the cells the message with the smallest timestamp(highest priority) will always receive the replies it is waiting for. Also since there is a timer determining how long a cell will wait for replies, there is no infinite waiting.

In a D-DCA algorithm, the channels act as the critical shared resource in the sense that, two or more cells, which are apart from each other closer than the Dmin, should not access the same channel concurrently. Since the DonorList Algorithm is ensuring no co-channel interference, the shared resource is not accessed concurrently. Therefore, with the features explained above, the DonorList algorithm is deadlock free.

4 Performance Evaluation

The performance of the DonorList algorithm is evaluated by extensive simulation studies with different C_t values and under various loads(see Table 1). The simulation program is written in Matlab v.6.5 R13[14] and implements the complete DonorList algorithm.

To evaluate the performance of the algorithm under realistic conditions, non-uniform traffic was applied. The non-uniform traffic was realized with two cell states; the normal state and the hot state[12]. The λ values for the given Erlang Loads are calculated by using the state diagram shown in Fig. 6 and equation (4). Mean cell-state change times are given in Table 1. Also, since the messages are transmitted through the wired network between the base stations, it is assumed that the message loss is negligible[2].

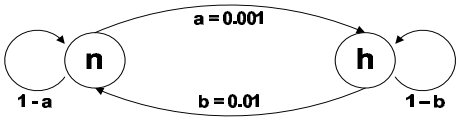


Fig. 6. Cell State Change State Diagram

$$Erlang = b/(a+b) * \lambda * T + a/(a+b) * 3\lambda * T \tag{4}$$

When in the normal state, a cell receives new calls with the exponentially distributed arrival rates λ and this arrival rate triples to 3λ when the cell enters the hot state [9],[12]. To eliminate the border effect, results were collected from the inner 121 cells to make sure that the cells that will provide the statistics have exactly 6 neighbors.

4.1 Message Complexity of the Proposed Algorithm

Let N be the number of cells in IN_i of any cell C_i. When the cell C_i needs to form its donor list, it sends N number of request and receives N number of reply messages.

On trying to import channels from the cells in its donor list, it sends k *acquire* messages to the cells holding the channel and receives k *confirm* messages, where k is the number of cells holding the channel. If the *confirm* messages are all with

Table 1. Simulation Parameters

Parameter	Value
Arrival rate in normal state	λ
Arrival rate in hot state	3λ
Mean call duration*(T)*	180 secs.
Probability of cell state change from normal to hot	0.001
Probability of cell state change from hot to normal	0.01
Ct	87%,95%
Erlang Loads	20,25,30,35,40,45,50
Time required to transmt and process a meassage	2 msecs[8],[9]

Table 2. Message Complexities

Algorithm	No of msgs. per allocation	Overall No. of. msgs.
D-CAT	3N+x	3N+x
DonorList	3dk	2N+3dk

"ok" the cell C_i sends k *release* messages to the cells which hold the channel, otherwise it sends k *keep* messages.

If the cell C_i cannot allocate a channel in the first hit, it repeats the above process d-1 times, where d is the number of accesses to the donor list, until it finds a channel to export.

So as a total of $2N+3dk$ messages are exchanged per channel export process. Table 2 shows the comparison between the message complexities of the D-CAT[12] and the proposed algorithm.

4.2 Results

In this section the simulation results, which are illustrated in Figure 7, will be discussed. For most of the results, the 95% confidence level for the measured data is less than 5% of the sample mean.

The performance results will be studied in terms of call incompletion probability, the channel utilization, mean number of messages per channel allocation and mean channel allocation delay under different traffic loads and various channel threshold values. Also, the call incompletion probability results will be compared with another threshold based distributed channel allocation algorithm, named as D-CAT[12], which proved to have a better call completion performance than [15],[16],[17].

The Figure 7a shows the call incompletion probability(P_{incomp}) results and their comparison with D-CAT. As illustrated in the Figure, as load increases P_{incomp} increases as expected. Under low load (Erlang 20 and 25), both the proposed DonorList algorithm and the D-CAT algorithm produces zero P_{incomp} values. For loads greater than Erlang 35 (i.e. at heavy load, which is the condition

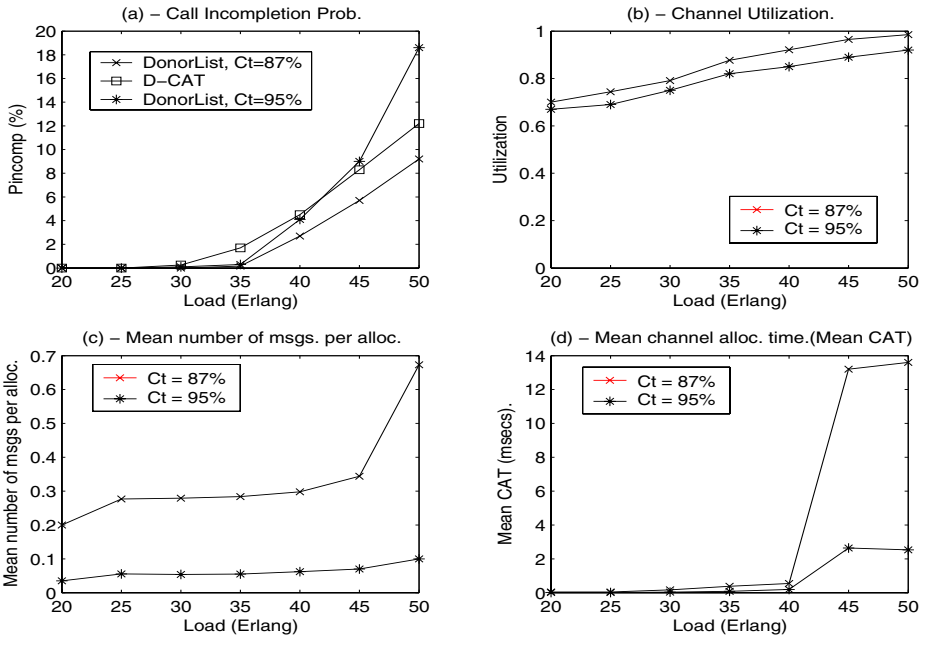


Fig. 7. Performance results

under which an algorithm demonstrates its performance strengths and weaknesses) and for $C_t = 87$, the proposed DonorList algorithm outperforms D-CAT by maintaining a P_{incomp} that is 30% lower on the avarage, than that of D-CAT algorithm.

The channel utilization performance is illustrated in Figure 7b. As seen in the figure, the utilization increases as load increases too. For $C_t = 87\%$, the channel utilization is always maintained above 70% and it reaches saturation ($\simeq 100\%$) at Erlang 50.

The mean number of messages per channel allocation results are shown in Figure 7c. As seen in the figure, the mean number of messages per allocation are always less than 1. Also, as given in table 2, the proposed algorithm never produces messages higher than 3N, where the D-CAT has 3N+x messages. This can be easily be proved by the fact that, in the proposed algorithm the value k can be maximum 3. Also, the simulation results show that the algorithm finds a channel to import in at most 2 donor list accesses (i.e. the value d can be maximum 2). Therefore, in the worst case, the maximum number of messages which will be produced by the proposed algorithm will be 2N+3dk where N=18, d=2 and k=3, which is equal to 54 messages. On the other hand, the D-CAT will have a 3N+x messages, which will be equal to 54+x. So, even under the worst case scenario, the number of messages produced by the proposed DonorList algorithm is lower than the number of messages produced by the D-CAT.

Figure 7d represents the mean time spent for each channel allocation. As seen in the figure, under all load values, the time spent for each channel allocation is lower than tolerable maximum delay, which is 100msecs[2]. The sudden increase seen when the system is heavily loaded (Erlang 45 and 50) can be explained as follows: Under heavy loads, all of the 144 cells will receive incoming calls very frequently. This causes an importer cell to successfully import a channel after the second access to the donor list or sometimes to block/drop the call. Therefore, under high loads, the worst case scenario explained in the previous paragraph occurs and since the number of massages reach the maximum, the time needed to send and process the messages increases as well.

Finally, for all the performance metrics discussed above, the proposed algorithm highly depends on the correct choice of the threshold value, C_t. If high C_t values are selected, the cells will not update their donor lists until a very high percentage of their channels become busy. This will result in low number of entries in their donor lists and high P_{incomp} values. Also, since the number of exporter cells will be low, at high C_t values, the number of messages per channel allocation and the mean channel allocation time will be lower.

On the other hand, at low C_t values, the entries in the donor list may become out of date (i.e. the reported available candidate channels may become busy).

The results show that the recommended C_t value for a stable and high-performance *DonorList* algorithm is 87%.

5 Conclusion

This paper presented a threshold based distributed channel allocation algorithm for cellular/wireless networks. The main goal of the study is to provide low call incompletion probabilities and high utilization and throughput values while keeping the number of messages for channel import processes as low as possible. The obtained results from extensive simulation studies prove that the algorithm succeeded in achieving the mentioned performance goals. Also the results show that the proposed algorithm overperforms the previously proposed algorithms in terms of the performance goals stated above. As the future work, adapting the algorithm for different service types (i.e. voice, video and data) and providing QoS to these services are being worked on. Also, the performance of the proposed algorithm under various user mobility conditions is a part of the current phase of this study.

References

1. Prakash, R., Shivaratri, N., Singhal, M.: Distributed dynamic fault-tolerant channel allocation for cellular networks. IEEE Transactions on Vehicular Technology **48** (1999) 1874–1888
2. Rappaport, T.S.: Wireless Communications-Principles and Practice. second edn. Prentice Hall, Upper Saddle River, NJ 07458 (2002)

3. Katzela, I., Naghshineh, M.: Channel assignment schemes for cellular mobile telecommunication systems: a comprehensive survey. IEEE Personal Communications **3** (1996) 10–31
4. Perros, H.G., Elsayed, K.M.: Call admission control schemes: a review. IEEE Communications Magazine **34** (1996) 82–91
5. Zhang, M., Yum, T.S.P.: Comparisons of channel-assignment strategies in cellular mobile telephone systems. IEEE Transactions on Vehicular Technology **38** (1989) 211–215
6. Prakash, R., Shivaratri, N.G., Singhal, M.: Distributed dynamic channel allocation for mobile computing. In: PODC '95: Proceedings of the fourteenth annual ACM symposium on Principles of distributed computing, ACM Press (1995) 47–56
7. Naghshineh, M., Schwartz, M.: Distributed call admission control in mobile/wireless networks. IEEE Journal on Selected Areas in Communications **14** (1996) 711–717
8. Dong, X., Lai, T.H.: Distributed dynamic carrier allocations in mobile cellular networks: search vs. update. In: ICDCS '97: Proceedings of the 17th International Conference on Distributed Computing Systems (ICDCS '97), IEEE Computer Society (1997) 108
9. Cao, G.: Integrating distributed channel allocation and adaptive handoff management for qos-sensitive cellular networks. Wirel. Netw. **9** (2003) 131–142
10. Gupta, S.K.S., Srimani, P.K.: Updatesearch: A new dynamic channel allocation scheme for mobile networks that can adjust to system loads. The Journal of Supercomputing **17** (2000) 47–65
11. Haung, Y.R., Ho, J.M.: Distributed call admission control for a heterogeneous pcs network. IEEE Trans. Comput. **51** (2002) 1400–1409
12. Zhang, Y., Das, S.K., Jia, X.: D-cat: an efficient algorithm for distributed channel allocation in cellular mobile networks. Mob. Netw. Appl. **9** (2004) 279–288
13. Lamport, L.: Time, clocks, and the ordering of events in a distributed system. Communications of ACM **21** (1978) 558–565
14. Mathworks: Matlab v6.5 R.13. http://www.mathworks.com (Last Visited: April 2005)
15. Cao, G., Singhal, M.: Efficient distributed channel allocation for mobile cellular networks. In: In the Proceedings of the IEEE 7th International Conference on Computers and Communication Networks, IEEE (1999) 50–57
16. Das, S., Sen, S., Jayaram, R.: D-lbsb: A distributed load balancing algorithm for channel assignment in cellular mobile networks. Journal of Interconnetion Networks **1** (2000) 195–220
17. Das, S., Y.Zhang: An efficient load-balancing algorithm based on a two treshold cell selection scheme in mobile cellular networks. Computer Communications **23** (2000) 452–461

QoS-Aware Video Communications over TDMA/TDD Wireless Networks*

Francisco M. Delicado, Pedro Cuenca, and Luis Orozco-Barbosa

Albacete Research Institute of Informatics
University of Castilla la Mancha
Campus Universitario s/n, 02071 Albacete, Spain
{franman, pcuenca, lorozco}@info-ab.uclm.es
Tlf.: +34-967-599200 ext 2497
Fax: +34-967-599224

Abstract. In recent years there has been an explosive growth on the use of wireless video communications. Despite much research in this field, the deployment of effective QoS-aware real-time video services over wireless channels remains a challenging task. In this paper, we first introduce and describe an overall system architecture capable of offering true end-to-end QoS guarantees to MPEG-4 video services running over TDMA/TDD wireless networks. The proposed system architecture is built by integrating two key system elements: a set of control mechanisms and various error resilient techniques. After reviewing the various system elements, we evaluate the use of the various mechanisms. We show the effectiveness of the proposed architecture in terms of various metrics. Our results show that the video quality as perceived by the end user can be significantly improved by making use of hierarchical video coding techniques.

Keywords: TDMA/TDD, WLAN, QoS, Hierarchical Video Coding, Multimedia Communications, Video Quality.

1 Introduction

In recent years, we have been witnessing an increasing interest in deploying wireless video communications. Despite much research in this field, the provisioning of QoS guarantees to real-time video over wireless channels remains a challenging task. Two major issues in providing true end-to-end wireless video capabilities are: mechanisms enabling the provisioning of QoS guarantees and the robustness of video compression algorithms operating over error-prone environments. From the point of view of the network, the main challenge when using VBR coded video is to guarantee the required quality of service (QoS). The deployment of

* This work was supported by the Ministry of Science and Technology of Spain under CICYT project TIC2003-08154-C06-02 and the Council of Science and Technology of Castilla-La Mancha under project PAI-06-0106.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 50–63, 2006.

proper control mechanisms both within the TDMA/TDD protocol architectures and the video application are needed to enable the deployment of effective digital video applications over wireless networks. This is due to the changing demands on resources, e.g., channel capacity and buffer space, needed for the transport of the video streams across the network as well as to the wireless channel characteristics. In order to overcome some of these problems, a set of control mechanisms have to be introduced into the protocol architecture of video communication systems.

Regarding the video application, video compression algorithms inherently remove redundancies making it more difficult to decode information under error and loss conditions. Major video coding standards make use of variable length code words and predictive frame coding aiming to significantly improve efficiency but at the cost of robustness. With variable length coding, packet losses can cause the decoder to incorrectly determine the length of a codeword leading to loss of synchronization in the decoding process. Since predictive coding techniques encode only the differences between frames or macroblocks, losses are much likely to propagate through the video stream thus degrading video quality. The effects of a packet loss will persist until non-predictively coded information occurs in the stream. In this work, we then show how error resilience techniques used in video compression algorithms can be used to improve the video quality. We argue that the final video quality perceived by the user can be significantly improved by the inclusion of hierarchical video coding techniques by sending the data into two separate streams. This allows the application to request various QoS guarantees from the video service, i.e., enabling the transmission of more sensitive data via a more reliable service.

We evaluate the effectiveness of our proposals in terms of the following metrics: network throughput, overhead, jitter, fairness and packet losses. A distinctive feature of our study is that we also validate the effectiveness of our proposed schemes by quantitatively evaluating the video quality as perceived by the end user.

The article is organized as follows. Section 2 provides a short overview of the operation of TDMA/TDD networks and describe a complete set of QoS mechanisms introduced in one of our previous work [1]. These mechanisms aim to provide the QoS guarantees required by time constrained applications when coexisting with other services. Section 3 describes techniques included in the MPEG-4 standard to increase robustness into the encoded video streams. A description of a hierarchical video coding technique for MPEG-4 is shown in this section. The results of our performance evaluation study are given in Section 4. Finally, Section 5 concludes the paper.

2 TDMA/TDD QoS-Aware Mechanisms

2.1 Principles of TDMA/TDD Networks

In a TDMA/TDD network the communications between all components of the networks is organized in frames. In each frame, the Base Station (BS) allocates

the time slots in response to the previous Subscriber Station (SS) requests. In this way, each SS has to request the required resources from the BS by issuing a *Resource Request (RR)* message, while the BS informs the SS of the positive outcome by using a *Resource Grant (RG)* message.

A normal TDMA/TDD frame is divided into four fundamental phases:

***Broadcast phase*:** this phase is used to carry out the overall frame control information. It contains the configuration parameters of the downlink and uplink phases, such as the positions and number of resources allocated to each active connection in each transmission phase. It is in this map that a control messages is typically included to convey the outcome of a successful resource request, i.e., a resource grant (RG) message.

***Downlink phase*:** it is the portion of frame which carries user data and control connections messages from the BS to the SS's.

***Uplink phase*:** similar to the downlink phase, this phase is formed by the user data and control messages associated to the uplink connections.

***Random Access phase*:** it is a portion of the frame which can be accessed by all SS´s using a contention process. This phase could be used by stations which have not been granted resources in the current frame to place their resource requests.

2.2 Resource Request Mechanisms

In one of our previous works [1], we have specified the following four different resource request mechanisms taking into account the QoS requirements of various types of applications:

Type 1: This mechanism is based on a contract. The contract is established after negotiation between an SS and the BS, at setup time. During this initial negotiation, the amount of resources to be granted to the SS are set. This type of resource request mechanism is suitable for applications characterized by a constant bit rate, such as, CBR-encoded voice services.

Type 2: Under this second type, the resource request mechanism is initiated by the BS through a *polling* mechanism. The BS polls the SS at the beginning of the connection allowing the SS to request the amount of resources it requires. The BS then polls once again the SS after having fulfilled the previous request or after a given time interval from the previous poll, whenever happens first. The length of the interval between polls should be set accordingly to the needs of the application.

Type 3: Under this request mechanism, the SS has to request its resources by sending a message using a contention process. Once having finished the allocation of the resources required by the SS, the BS, similarly to the Type 2 mechanism, polls the SS.

Type 4: The main difference between this type with respect to the Type 3 request mechanism comes from the fact that regardless of the activity of the connection, the SS has to go through a contention process in order to place

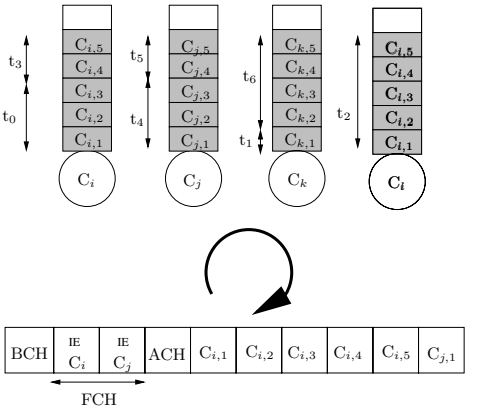


Fig. 1. Bandwidth allocation scheme operation

its resource request. In particular, different to the previous type, Type 3, once the BS has finished fulfilling the SS requirement, the SS has to go once again through a contention cycle to place its request.

2.3 Bandwidth Allocation Schemes

The BS has as one of its main duties the implementation of the actual bandwidth allocation scheme. Since there is one message in the broadcast phase per each connection, the amount of overhead introduced into the frame will heavily depend on the way the resources are assigned to the various connections. However, this allocation should not penalize the ability of providing the QoS requirements to the various applications.

These two factors: the amount of overhead introduced for the mechanism to operate and the traffic differentiation capabilities were studied by us in [2]. In that study, we introduced a novel scheme addressing these two issues, namely, the Minimum Overhead Round Robin (MORR) scheme. The main aim of the MORR scheme is to limit the amount of overhead to be introduced in the frame by contiguously allocating the channels to a given connection. The mode of operation of the MORR mechanisms is depicted in Figure 1, where (t_i) denotes the arrival time of the requests, and a queue is assigned to each one of the active connections. For the purpose of this work, we will further enhance this scheme by integrating a two-level priority policy at each queue. This policy should be particularly useful when dealing with hierarchical encoded video streams.

3 MPEG-4 Error Resilience Tools

As already stated, the fact that the MPEG-4 video coding scheme uses compression techniques makes any MPEG-4 based video communications application very vulnerable to packet losses. In the absence of any error propagation control

mechanism, the loss of each unit of information may cause the loss of information up to the next synchronization point, e.g., Video Object Plane-VOP headers. In other words, a packet loss in the coded video bit-stream will result on the loss of all the macroblocks that follow up to the end of the current VOP. This phenomenon is known as spatial impairment propagation. Furthermore, due to the predictive nature of the MPEG-4 algorithm, when errors or losses occur in an I or P-VOP, the VOPs encoded using as reference the affected I or P-VOP will not be properly decoded. The losses will propagate until the next intra-coded VOP; this is referred to as temporal impairment propagation.

To address these issues the MPEG-4 video standard defines a set of special error resilience tools [3]. The standard supports flexible re-synchronization markers and data partitioning features to separate motion and header information from texture information and reversible variable length coding.

3.1 Video Packet Resynchronization (VP)

Video packet resynchronization is an approach aiming to reduce the spatial propagation of errors. This approach consists in introducing resynchronization markers into the bit-stream. Whenever the decoder detects an error, it can then look for the following resynchronization marker and quickly regain resynchronization. According to the specifications of the MPEG-4 standard, the resynchronization markers can be periodically inserted every K bits; this scheme divides the bit-stream into data packets that are independent from each other named Video Packets (VP). At the beginning of each video packet, the encoder inserts two additional fields in addition to the resynchronization markers to remove all data dependencies between the data belonging to two different video packets. These are: the absolute macroblock number of the first macroblock in the video packet (MB number), which indicates the spatial location of the macroblock in the current VOP; and the quantization parameter (Q_p) used to quantize the DCT coefficients.

3.2 Data Partitioning (DP) - Hierarchical Video Coding

The Data Partitioning (DP) error resilience tools defined by the MPEG-4 standard specifies that each I or P-VOP video packet can be divided into two different partitions. The first one (the most important part of the video packet) contains the header, which encodes the information pertaining to the first macroblock of the video packet and the HEC extension, if used, shape data, the motion information (for P-VOP´s) or DC coefficients (for I-VOP´s) of the macroblocks. The second partition contains the AC's coefficients of the macroblocks, for I-VOP´s, and the texture information for P-VOP´s. If the second partition is lost during transmission, the MPEG-4 decoder can decode the video packet using only the first partition. In [4], we have shown that extending this hierarchical encoding scheme to the B-VOP´s proves effective in enhancing the robustness of the video encoded stream. We then consider its use in this work.

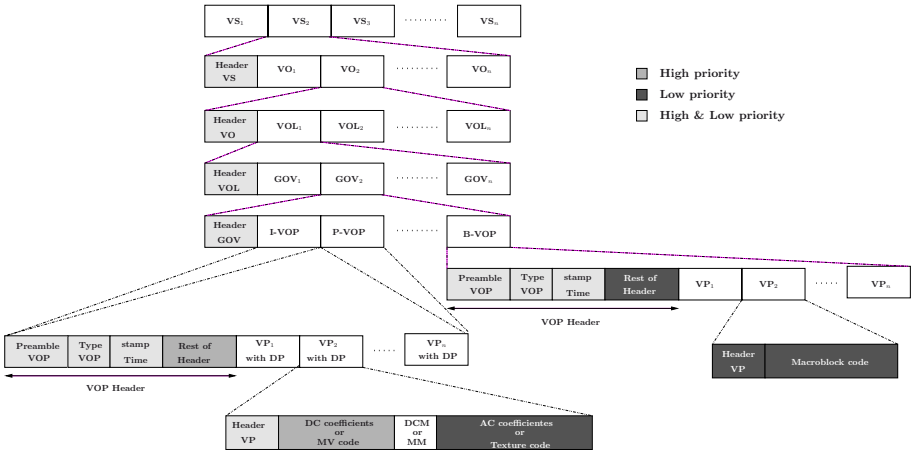


Fig. 2. Hierarchical MPEG-4 Video Coding Scheme proposed

In order to actually transmit the encoded video stream using the DP tools, we prioritize the transmission of the first partition over the second one. Towards this end, we will consider that the aforementioned bandwidth allocation mechanisms implement a priority discipline. In this way, whenever a high priority packet (pertaining to the first partition) be present in the output queue, this one will be first sent over the wireless link. This mechanism should reduce the possibility of losing high-priority video packets due to excessive delays in accessing the channel. However, in order for the decoder to be able to reconstruct the video stream, we have to include the VOP start code, the type of VOP and the time stamps into the second partition; the low priority video stream. To ensure synchronization within VOP, the resynchronization marker of the video packet and the number of the first macroblock have also to be copied into the video packet of the low-priority partition. It should be clear that this scheme, referred from now on as Hierarchical Video Coding, adds some extra overhead traffic by requiring the duplication of some parts of the video data. The actual amount of overhead will depend on the particular setup characteristics. In the system being considered throughout our simulations, the overhead introduced by adding this feature is approximately 1.2% of the total video data with respect to the non-hierarchical encoded video.

3.3 Reversible Variable Length Codes (RVLC)

RVLC can be used in conjunction with the aforementioned data partitioning tools to recover more DCT data from a corrupted texture partition. RVLC's are designed such that they can be decoded both in the forward and in the backward direction. If the decoder detects an error while it is decoding the texture part in forward direction, it looks for the next resynchronization marker (start of the

next video packet), and then decodes the texture part in the backward direction until an error is detected. Based on the two errors location, the decoder can recover some of the data that would have otherwise been discarded.

4 Performance Evaluation

In order to evaluate the proposed mechanisms, we have developed a simulator using OPNET 10.0 [5]. This simulator has been developed using the frame structure of HIPERLAN/2. In our simulations, we use one HIPERLAN/2 cell operating in centralized mode supporting four types of service: voice, video, best-effort and background. In the composition of the frame we use short preambles, guard times of 2 μs, the random access phase is formed by three transmission slot and the physical mode for the control and data user messages are QPSK-3/4 (18 Mbps) and 16QAM-9/16 (27 Mbps), respectively.

Given that one of the main objectives of this study is to evaluate the performance and effectiveness of the proposed system architecture, we have considered out two main scenarios. Under the first scenario, namely Scenario without QoS, all applications have to go through a contention-based process when attempting to transmit each and every resource request packet. Under the second scenario, Scenario with QoS, each of the applications makes use of a different type of mechanism. The following has been used: voice services make use of the Type 1 mechanism with 48 bytes reserved every 12 frames (this corresponds to a guaranteed data rate of 16 Kbit/s). Video services make use of the Type 2 mechanism with a timer period of 40 *ms*. The value of this latter parameter has been derived based on the results obtained in our previous studies. The best-effort (BE) and background traffic (BK) make use of the Type 3 and Type 4 mechanisms, respectively.

The voice traffic is implemented using a constant bit-rate voice source encoded at a rate of 16 Kbits/s according to the G.728 standard [6]. The voice sources are randomly activated within the first 24 *ms* of the simulation. The video traffic has been characterized by MPEG-4 [3] video traffic traces. Each video application begins its transmission within a random period given by the expression $t = uniform(0, \frac{12}{f})$ being f the video frame rate. In this way, the peak periods of the source rates are randomly distributed along a Group Of Pictures (GOP) period. The transmission of a video frame is uniformly distributed along the interval of duration of a frame ($\frac{1}{f}$). We use the sequence *Funny* encoded on CIF format at 25 frames/s. The video sequence has been encoded using the DP scheme and integrating the RVLC scheme with Video Packets of 768 bits. We consider, both, the transmission of the video sequence using the same priority levels for the two partitions, referred as the non-hierarchical case, and by using a hierarchical transmission scheme, i.e., two levels of priority. The best-effort traffic is generated using the traffic model for Web surfing applications described in [7]. The background traffic generated by each source is a combination of FTP, e-mail and Napster according to the model described in [8]. The traffic sources of these two latter traffic types are initiated at the beginning of the simulation run.

All connections are assumed to be running in both directions, i.e., uplink and downlink. In order to carry out this study, we have considered that one third of the SS's will be running voice/video applications. Another third of the SS's generate best-effort traffic and all the other SS's generate background traffic. We start by simulating a wireless network consisting of three SS's. We then gradually increase the *Total Offered Load* of the wireless LAN by increasing the number of SS's by three. In this way, the stations are always incorporated into the system in a ratio of 1:1:1 for voice/video, best-effort and background, respectively. We increase the number of terminals on a three by three basis starting at 3 and up to 18 stations. In this way, the normalized offered load is increased from 0.16 up to 1.2. We have preferred to evaluate a *normalized* offered load, rather the absolute value. The normalized offered load is determined with respect to the theoretical maximum capacity (27 Mbps).

4.1 Metrics

In our study, we have been interested in assessing the performance in terms of the following metrics: total normalized throughput, overhead, jitter distribution, packet loss rates, packet loss distribution, fairness and video quality.

The analysis of the *total normalized throughput* shows the utilization of the wireless medium. This metric refers to the percentage of the total offered data (the traffic from all the sources) that is actually delivered to the destination. It should be clear that this metric lies within the interval [0,1]. When this metric is less than 1, this fact indicates us that the presence of packet losses.

In order to provide us a clear indication of how the capacity of the channel is being used, the *overhead* metric is evaluated. It is a relative measure and it is simply defined as the ratio between the control bits and the total number of bits (data plus control) being sent, i.e., composing the frame. It should be clear that at low loads, there may be some spare capacity, i.e., the frame is not completely filled up.

In order to limit the delay experienced by the voice and video applications, an essential condition to guarantee the QoS required by both applications, the maximum time that a unit of voice and video may remain in the transmission buffer has been set to 10 *ms* and 100 *ms*, respectively. These time limits are in line with the values specified by standards and in literature [9]. A packet exceeding this upper bound is dropped. The loss rate due to this mechanisms is given by the *Packet Loss Rate (PLR)*.

An important measure when evaluating packet loss rates for applications particularly sensitive to the packet loss, like MPEG-4 video compressed applications, is the *length of a loss burst* (L_{burst}) and the *distance between bursts*(D_{burst}). We evaluate this loss distribution using the CDF. It is well known that the quality of the video sequence heavily depends on the loss pattern. In particular, a long burst will make it practically impossible for the decoder to recover the information. On the contrary, in the presence of short loss bursts, a decoder may be able to reconstruct part of the lost information through the use of the RVLC scheme.

One of the most important metrics in multimedia communications is the quality of the received video sequence. This has been evaluated using the Moving Picture Quality Metric (MPQM) [10]. This metric has proved to behave consistently with the human judgments, i.e., according to the quality scale that is often used for subjective testing in the engineering community (see Table 1).

Table 1. Video Quality Scale

Rating	Impairment	Quality
5	Imperceptible	Excellent
4	Perceptible, not annoying	Good
3	Slightly	Fair
2	Annoying	Poor
1	Very annoying	Bad

Finally, we evaluate the fairness of the allocation schemes between flows of the same type (voice, video, best-effort and background). For this purpose, we calculate the *Fairness Index* (FI) defined in [11]. This index is defined as:

$$FI = \frac{(\sum_{i=1}^{n} T_i)^2}{n \times \sum_{i=1}^{n} (T_i)^2},$$

where n is the number of the same type flows, and T_i is the throughput of the flow i. Recall that $FI \leq 1$, and it is equal to 1 if all T_i are equal, which corresponds to the highest degree of fairness between the different users.

In the simulation results, each point in the plots is an average over forty simulation runs, and the error bars indicate the 90% confidence interval. Moreover, our measurements started after a warm-up period allowing us to collect the statistics under steady-state conditions.

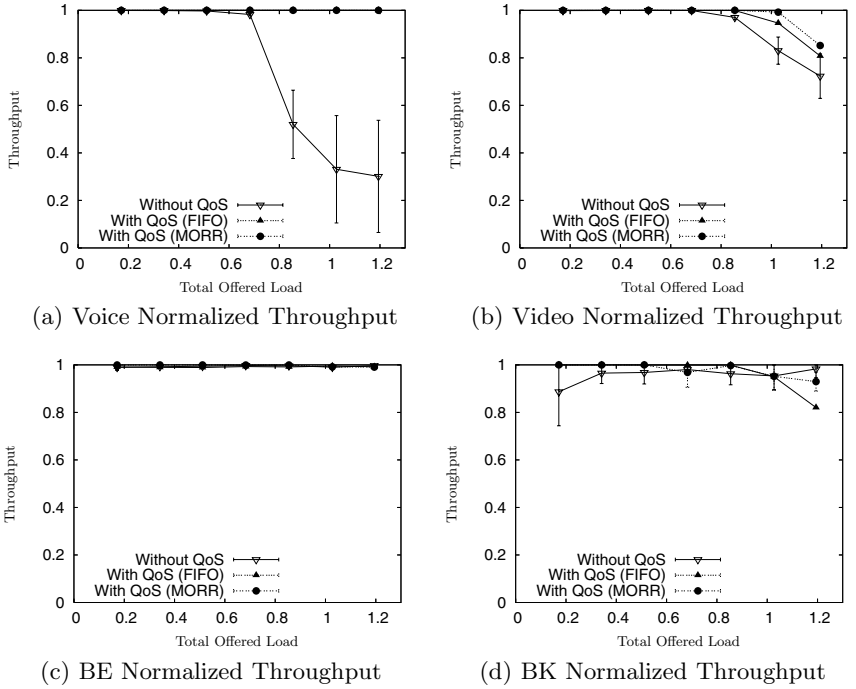
4.2 Simulation Results

Figure 3 represent the normalized (carried) throughput by type of traffic as a function of the offered load for both scenarios, with and without QoS, and in the case of use QoS using two allocation algorithms, FIFO and MORR. For voice traffic, Figure 3.(a), it is appreciated that in the scenario with QoS, all the traffic is served independently of the load. This is due to the fact that the Type 1 request method consists in contract all the resources need for this connections. In the case when all the requests are sent using a contention process, the performance decreases rapidly as soon as the load exceeds 50% of the network capacity.

The worst performance for Throughput of video traffic is obtained for the case of the scenario without QoS, Figure 3.(b). The priorization of video request using the Type 2 request mechanism proves effective, particularly when using the MORR scheme. The figure shows that all the video traffic can be effectively served up when the MORR allocation scheme is used. The MORR proves

more effective in differentiating the video traffic. Figures 3.(c) and (d), represent the throughput for the best-effort and background traffic, respectively. The performance is very similar for all system configuration, except for the slight penalization suffered by the background traffic at high network loads when using the QoS mechanisms. This is due to the fact that the control schemes effectively favor the video traffic over the lowest priority traffic, i.e., the background traffic.

Figure 4 depicts the overhead as a function of the offered load for the three bandwidth allocation schemes under study. As seen in the figure, the overhead decreases as the load is increased for all cases and for loads up to 50%. For the case of the FIFO mechanism, the overhead introduced in the frame is lower under Scenario without QoS than in Scenario with QoS. This difference is due to the mechanism used to place the requests and the policy used to serve the requests. Remember that under Scenario without QoS, the SS´s make use of a contention-based process to place their requests. As the load increases, the SS's spend more time attempting to place their requests. As the number of channels requested is being updated during this period of time, a larger number of channels will be requested. Furthermore, since the requests are served following a FIFO policy, the overhead decreases as the number of actual channels used to convey user data is increased.



(a) Voice Normalized Throughput (b) Video Normalized Throughput

(c) BE Normalized Throughput (d) BK Normalized Throughput

Fig. 3. Normalized Throughput for all Connection Types

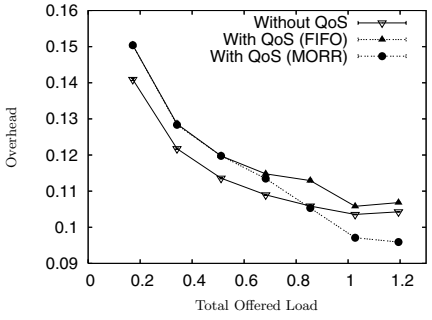
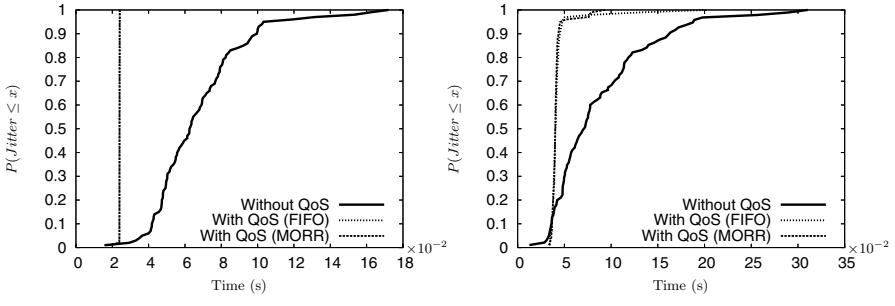


Fig. 4. Overhead



(a) CDF - Voice Jitter. (b) CDF - Video Jitter.

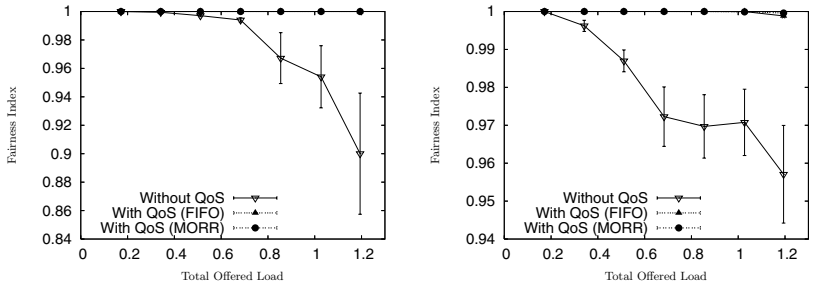
Fig. 5. CDF of Jitter for Voice and Video Connections (Offered Load≅ 100)

Figure 4 shows that the system combining the contention based procedure and the bandwidth allocation scheme based on a simple FIFO scheme (Scenario without QoS) provides the best results for loads up to 80%. However, as the system is exposed to higher loads, the use of a contentionless process and a more intelligent bandwidth allocation scheme proves to be more efficient.

Regarding the jitter, Figure 5.(a) shows that voice communications do not suffer any deviation since a static allocation of resources ensure the isochronous transmission of the voice packets, one voice packet every 24 *ms*, independently of the network load conditions.

In the case of the video traffic (Figure 5.(b)), the jitter remains constant for Scenario with QoS when using FIFO and MORR mechanisms. The figure shows that 95% of the inter-arrival times between frames are 40 *ms*. This corresponds to the sampling rate of 25 frames/*s*, i.e., a frame every 40 *ms*. This is an excellent result that indicates clearly the effectiveness of the proposed mechanisms.

The Fairness Index of voice and video is shown in Figure 6. In this case, Scenario without QoS shows the worst performance results mainly due to the use of a contention process. In the case of Scenario with QoS, there are not differences between the results obtained using the different allocation schemes under study.



(a) Fairness Index of Voice. (b) Fairness Index of Video.

Fig. 6. Fairness Index of Voice & Video

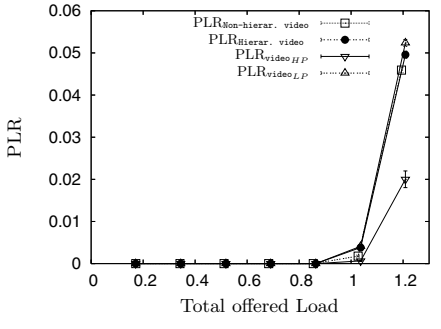
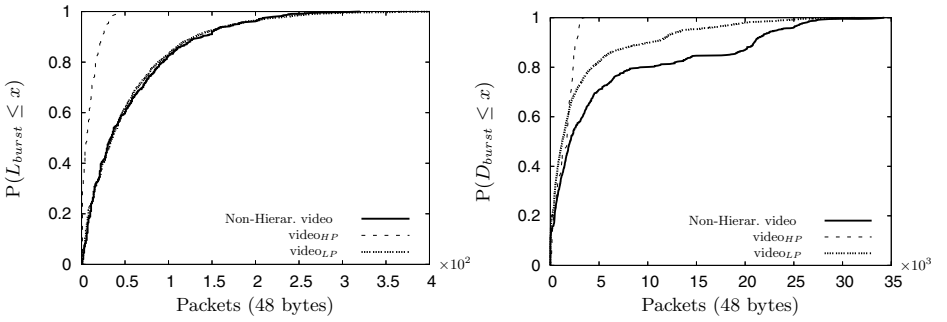


Fig. 7. PLR - Normal and Hierarchical video

To evaluate the performance of the hierarchical video coding, we have used a normal video stream and a hierarchical version of the same sequence and making use of the MORR allocation schemes. We denote by $video_{HP}$ the high priority layer stream of the hierarchical video, and $video_{LP}$, the low priority video layer stream. Figure 7 depicts the loss rates for the normal and hierarchical encoded video. The figure also distinguishes between the packet loss rates of the low and high priority layers of the hierarchical video stream. Obviously, the PLR of the overall hierarchical video is higher than the PLR of the normal video, since the hierarchical process introduces an overhead of 1.19% into the output stream. As expected, the results show that the low priority video exhibits a higher loss rate when compared to the loss rate experinced by the high priority traffic.

Figure 8.(a) shows the CDF of the size of loss bursts. From the results, it is clear that the loss burst exhibits similar size in the cases of the overall video encoded using the DP tools of the MPEG-4 standard and the low priority layer of the hierarchical video: both being higher than the burst size for the high priority layer. A similar trend is shown in the case of the CDF of the distance between loss bursts, see Figure 8.(b). This can be simply explained by realizing that the low priority video represents 91.75% of the hierarchical video traffic while only the remaining 8.25% belongs to the high priority video layer.



(a) CDF of size of video burstlosses, load ≈100%.

(b) CDF of distance between losses video burst, load ≈100%.

Fig. 8. Pattern of Losses in Hierarchical and non-Hierarchical Video

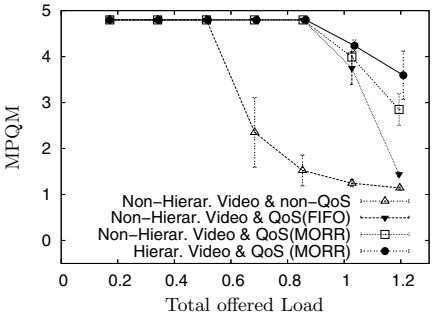


Fig. 9. Quality of Hierarchical and Non-hierarchical Video

To summarize the performance evaluation results, Figure 9 represents the decoded video quality when integrating the different techniques introduced herein. The figure shows that using a resource request algorithm adapted to each type of traffic proves effective for network loads of up to 80%. The figure also shows that the quality can be further improved by using a bandwidth allocation mechanism which minimizes the overhead and making use of a hierarchical video transmission versus a non-hierarchical video transmission.

5 Conclusions

In this article, we have evaluated a set of QoS mechanisms and the MPEG-4 error resilience tools as a means of deploying effective video services over TDMA/TD wireless networks. Through an extensive campaign of simulations, we have evaluated the capabilities of the overall protocol architecture in terms of various metrics. In particular, we have shown the effectiveness of our proposals in terms of the video quality as perceived by the end-user.

References

1. F. Delicado, P. Cuenca, L. Orozco-Barbosa, and A. Garrido, "Design and Evaluation of a QoS-aware Framework for Wireless TDMA/TDD," *Wireless Personal Communications Journal*, vol. 2005, no. 34, pp. 37–90, 2005.
2. F. Delicado, P. Cuenca, and L. Orozco-Barbosa, "QoS Mechanisms for Multimedia Communications over TDMA/TDD WLANs," *to be published in Computer Communications Journal*, 2006.
3. *Information Technology- Generic Coding of Audio-visual Objects- Part 2: Visual*, ISO/IEC Std. 14 496-2, March 1999.
4. F. Delicado, A. Garrido, P. Cuenca, L. Orozco-Barbosa, and F. Quiles, "Improving the Robustness of MPEG-4 Video Communications over Wireless/3G Mobile Networks," in *Proc. of 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'02)*, vol. 4, Lisbon, Portugal, September 2002, pp. 1685–1689.
5. *OPNET Modeler 10.0*, © 1987-2003 OPNET Technologies, Inc., http://www.opnet.com.
6. *Coding of Speech at 16 Kbit/s Using Low-delay Dode Excited Linear Prediction*, ITU-T Std. Rec. G.728, September 1992.
7. G. Colombo, L. Lenzini, E. Mingozzi, B. Cornaglia, and R. Santaniello, "Performance Evaluation of PRADOS: a Scheduling Algorithm for Traffic Integration in a Wireless ATM Networks," in *Proc. of ACM MOBICOM'99*, Seattle, WA, August 1999, pp. 143–150.
8. A. Klemm, C. Lindemann, and M. Lohmann, "Traffic Modeling and Characterization for UMTS Networks," in *Proc. of IEEE GLOBECOM'01, Internet Performance Symposium*, San Antonio, TX, November 2001.
9. A. Karam and F. Tobagi, "On the Traffic and Service Classes in the Internet," in *Proc. of IEEE GLOBECOM'00*, San Francisco, CA, USA, 2000.
10. C. J. Van den Branden and O. Verscheure, "Perceptual Measure Using a Spatio-Temporal Model of Human Visual System," *Proceedings of SPIE Conference on Electronic Imaging, Digital Video Compression: Algorithms and Technologies*, vol. 2668, pp. 450–461, San Jose, January 1996.
11. J. R., A. Durresi, and G. Babic, "Throughput fairness index: An explanation," ATM Forum/99-0045, Tech. Rep., Feb 1999.

Channel State-Aware Joint Dynamic Cell Coordination Scheme Using Adaptive Modulation and Variable Reuse Factor in OFDMA Downlink

Dae Wook Byun, Young Min Ki, and Dong Ku Kim

Yonsei University, Dept. of Electrical and Electronic Engineering
134 Shinchon-Dong, Seodaemun-Gu, Seoul 120-749, Korea
{ladiosop, mellow, dkkim}@yonsei.ac.kr
http://mcl.yonsei.ac.kr

Abstract. In this paper, two different dynamic cell coordination stratagies for frequency selective and flat fading are proposed for efficient subcarrier allocation in the joint consideration of adaptive modulation and variable frequency reuse in the channel-aware OFDMA downlink multicellular environment. Compared to a conventional OFDMA system without cell coordination, where system throughput may become degraded due to the persistent interference from other cells, the proposed system dynamically allows RNC to apply different reuse factors on each subchannel and scheduling in consideration of channel and interference conditions of individual users so as to increase the system throughput and guarantee QoS of each user. In a selective fading channel, the proposed schemes showed 2.6 times as large throughput as that of a single reuse factor of one for all subcarriers. In a frequency flat fading, the dynamic scheme with the proposed scheduling achieves on average three times larger throughput than the conventional dynamic scheme [8].

1 Introduction

Future wireless communication system designs will require support for high data rates, provision of various quality of services (QoS) for multiple users, and operation in a multipath radio channel environment. Orthogonal frequency division multiple access (OFDMA) was proposed as one of the most promising technologies believed to satisfy most of these demands.

In either OFDMA or OFDM systems, one of the important issues is efficient subcarrier allocation to users. Some dynamic subcarrier allocation algorithms [1][3][4] were proposed for the multiple types of services that require various data rates. However, most of the algorithms were not considered in a multicell environment. An inter-cell interference avoidance technique was proposed [5]. A key consideration in designing a multicell cellular environment was frequency reuse, which is the ability to use the same frequencies repeatedly. A reuse scheme was proposed that divides a cell into several concentric zones in which

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 64–75, 2006.

each zone is assigned a different frequency reuse factor [6][7]. This scheme can be easily implemented but can not efficiently adapt time variation of mobile distribution and channels. Therefore, both frequency reuses and channel scheduling should be considered jointly for more efficient subcarrier allocation in a multicell environment.

Simplified Subchannel Allocation Scheme (SSAS) [8] were proposed by considering frequency reuse and adaptive modulation in the cellular OFDMA system in frequency flat fading. However, since its performance is degraded in practical environment priority based greedy schemes are proposed to enhance performance. In the case of frequency selective fading, the proposed cell coordination schemes achieves better performance than the static cell coordination scheme, considering different channel gain of each subchannel.

The remainder of the paper is organized as follows. In Chapter 2, the concept of frequency reuse and the system model are described, and the performance of the system using the single reuse factor is investigated. In Chapter 3, the dynamic cell coordination scheme [8] is reviewed and the proposed dynamic cell coordination schemes are introduced in frequency flat fading environment. In Chapter 4, novel dynamic cell coordination schemes are introduced in more detail in conjunction with frequency selective fading. In Chapter 5, the performance of the proposed schemes is demonstrated. Finally, conclusions are presented in Chapter 6.

2 System Model and No Cell Coordination

2.1 Reuse Factor and System Model

A subchannel is defined as a group of adjacent subcarriers. The frequency reuse factor used in this paper is slightly different in that each cell of a cluster is allowed to access whole subchannels in the system and each subchannel of each cell can be assigned with different reuse factors. Hence, all subchannels in a cell are not always exploited in a cell unless the reuse factor of all subchannels is 1.

Consider a downlink OFDMA system using adaptive modulation and coding (AMC) in a multicell environment of 37 hexagonal cells of 1km radius for the reuse factors of 1, 3, and 7. It is assumed that pilot signal contains base station (BS) index so that mobile station (MS) distinguishes pilots from each BS and estimates each different SINRs for corresponding reuse factors that could be used in the system. Each subchannel is assigned one of the reuse factors by schemes shown later on. The allocated power of each subchannel is assumed to be equal and the identical modulation scheme is applied to subcarriers within a subchannel. Parameters such as symbol duration and frequency offset are assumed to be designed such that inter-symbol interference and inter-channel interference can be neglected.

2.2 No Cell Coordination with Single Reuse Factor

The reuse factor of each subchannel is predetermined by the system. MS measures SINRs value and determines the transmittable data rates of the subchannels,

which are transmitted to BS through feedback channel. BS receives the data rates of each subchannel from each MS and allocates subchannels according to the proportional fairness (PF) scheduling algorithm. The selection of users in the PF scheduling algorithm is well known as

$$i_n^* = \arg\max_i \frac{R_{i,n}(t)}{\overline{R_{i,n}}(t)}, \tag{1}$$

where $\overline{R_{i,n}}(t)$ and $R_{i,n}(t)$ denote the average and the instantaneous data rates of the n-th subchannel of user i, respectively. PF scheduling is performed independently in each subchannel.

2.3 The Performance in Using Single Reuse Factor

1) *Comparison of cell throughput*: Fig. 1(a) illustrates the comparison of cell throughput for various reuse factors in frequency flat and frequency selective fading, where RF k denotes reuse factor k. Among various reuse factors, it is easy to expect that the cell throughput for reuse factor of one is the largest. Cell throughput on frequency flat fading is higher than that of frequency selective fading, which has been shown in many other literatures.

2) *Comparison of fairness*: Fig. 1(b) illustrates the comparison of fairness for different reuse factors when the numbers of users are 5 and 15, where it is easily expected that fairness performance is improved by using larger reuse factor.

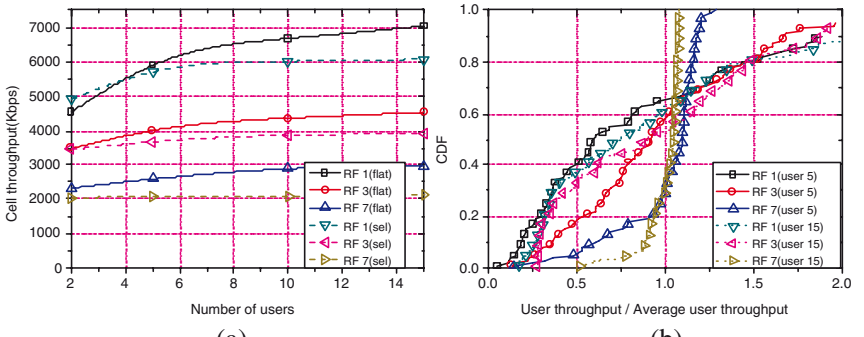


Fig. 1. (a) Cell throughput comparison in frequency flat and selective fading; (b) Comparison of fairness for reuse factors of 1, 3, and 7

3 Dynamic Cell Coordination for Frequency Flat Fading

3.1 Static Cell Coordination

In static cell coordination, radio network controller (RNC) determines the reuse factors of each subchannel, where the resultant reuse factors of each subchannel

does not change throughout the transmission time. BS allocates the subchannel of certain reuse factors determined by RNC to users with a certain scheduling algorithm.

Only three different values of reuse factors, which are 1, 3, and 7, are considered. The numbers of the subchannel of each reuse factor is denoted by a/b/c, where a is the number of subchannels of reuse factor of 1, b for 3, and c for 7. Three different frequency allocation, which are (22/1/1), (9/3/2), and (1/1/4), are considered, where (22/1/1) is one using the reuse of one dominantly, (9/3/2) for the reuse of three dominant, and (1/1/4) for the reuse of seven dominant.

3.2 Priority Based Greedy Cell Coordination Scheme

Priorities of Users

1) The priority using spectral efficiency: A spectral efficiency of a subchannel is defined as ratio of transmittable data rate of user to reuse factor [8]. The priority of the user i is computed by using spectral efficiency as follows:

$$\text{Priority of user } i = \frac{R_k^{ib}}{k}, \tag{2}$$

where R_k^{ib} is the achievable data rate of a subchannel with reuse factor k for user i in BS b. The highest priority is assigned to the user with the highest spectral efficiency per subchannel. Therefore, users having good channel condition are served more often, while those users having bad channel condition are served infrequently.

2) The priority using the spectral efficiency and the average user throughput: The priority of user is determined by considering $\overline{R}^{ib}$ as follows:

$$\text{Priority of user } i = \left(\frac{R_k^{ib}}{k}\right) \Big/ \overline{R}^{ib}, \tag{3}$$

where $\overline{R}^{ib}$ represents the average data rate of a subchannel for user i in BS b. Unlike the case described by (2), (3) generates the spectral efficiency normalized by its average data rate, which is more fair than spectral efficiency itself.

Priority Based Greedy Cell Coordination Schemes

The proposed schemes offer three different ways of calculating the number of required subchannels of cells without changing function of RNC that was shown in SSAS [8], where the allocation of subchannels is done every frame in BS.

1) Priority based greedy cell coordination scheme 1: According to the R_k^{ib} of each user, the number of the required subchannels is obtained as follows:

$$R_k^{ib} \cdot N_k^{ib} \geq T_i^b, \tag{4}$$

where N_k^{ib} and T_i^b denote the number of required subchannels and the predetermined required data rate for user i in BS b, respectively. The scheme allocates subchannels in greedy manner while guaranteeing T_i^b during every frame.

2) Priority based greedy cell coordination scheme 2: It calculates N_k^{ib} by using both average and the instantaneous data rate of user i such that QoS does not need to satisfy T_i^b within every frame but does in average sense. The number of the required subchannels of each user is computed as follows.

$$\left(\frac{N-1}{N}\right) \cdot \overline{R}^{ib} + \frac{1}{N} \cdot R_k^{ib} \cdot N_k^{ib} \geq T_i^b, \tag{5}$$

where N represents the moving window size used to evaluate the average data rate of user i.

3) Priority based greedy cell coordination scheme 3: It is basically similar to scheme 2 except that all surplus channels at each BS are assigned to the user with the highest priority.

4 Cell Coordination for Frequency Selective Fading

4.1 Static Cell Coordination

Static cell coordination in a selective fading is the same as in flat fading except that scheduling algorithm should be performed for each subchannel basis.

4.2 Spectral Efficiency and Priority Based Dynamic Cell Coordination

In the application of a frequency selective fading, in which channel gains are constant over a subchannel and independent of each subchannel, the amount of feedback information of channel condition to BS increases. An important observation is demonstration of the efficiency of the proposed coordination schemes with which subchannels are assigned multiple reuse factors to minimize intercell interference with priority of users.

Two schemes are proposed: the dynamic maximum C/I cell coordination (DMCC) scheme and the dynamic proportional fairness cell coordination (DPFCC) scheme. In DMCC, subchannels are allocated to users by considering the spectral efficiency of users within each BS. In DPFCC, the spectral efficiency is replaced by the priority of users using an average user throughput. The proposed cell coordination schemes are composed of the following steps.

1) *MS report*: MS measures three values of SINR assuming reuse factors of 1, 3, and 7 for each subchannel. The transmittable data rate at each subchannel is calculated from the measured SINRs and the corresponding spectral efficiencies are determined as follows.

$$e_{k,n}^{ib} = \frac{R_{k,n}^{ib}}{k} \tag{6}$$

$$k_{best,n}^{ib} = \arg\max_k e_{k,n}^{ib}, \tag{7}$$

where $e_{k,n}^{ib}$ denotes the spectral efficiency of the n-th subchannel of user i in BS b with reuse factor of k. MS transmits $k_{best,n}^{ib}$ and $e_{k_{best},n}^{ib}$ values to BS.

2) *BS report*: In DMCC, the b-th BS gathers $k_{best,n}^{ib}$ and $e_{k_{best},n}^{ib}$ values from users and creates the matrix $\mathbf{Q}^b$ which is formed by

$$\mathbf{Q}^b = \begin{pmatrix} e_{1,1}^{\hat{i}b} & e_{1,2}^{\hat{i}b} & \cdots\cdots & e_{1,n}^{\hat{i}b} \\ e_{3,1}^{\hat{i}b} & e_{3,2}^{\hat{i}b} & \cdots\cdots & e_{3,n}^{\hat{i}b} \\ e_{7,1}^{\hat{i}b} & e_{7,2}^{\hat{i}b} & \cdots\cdots & e_{7,n}^{\hat{i}b} \end{pmatrix}, \tag{8}$$

where $\hat{i}(k,n,b) = \arg\max_{i:\hat{k}=k} e_{\hat{k},n}^{ib}$ and $\hat{i}$ denotes user who has the maximum spectral efficiency at the n-th subchannel with reuse factor k in BS b. An element of the matrix $\mathbf{Q}^b$ has the largest spectral efficiency among the n-th subchannel of the same reuse factor of all users in BS. In DPFCC, the priority of users is evaluated as follows.

$$p_{k_{best},n}^{ib} = \frac{R_{k_{best},n}^{ib}}{\overline{R}^{ib}} \tag{9}$$

$$\mathbf{Q}^b = \begin{pmatrix} p_{1,1}^{\hat{i}b} & p_{1,2}^{\hat{i}b} & \cdots\cdots & p_{1,n}^{\hat{i}b} \\ p_{3,1}^{\hat{i}b} & p_{3,2}^{\hat{i}b} & \cdots\cdots & p_{3,n}^{\hat{i}b} \\ p_{7,1}^{\hat{i}b} & p_{7,2}^{\hat{i}b} & \cdots\cdots & p_{7,n}^{\hat{i}b} \end{pmatrix}, \tag{10}$$

where $\hat{i}(k,n,b) = \arg\max_{i:\hat{k}=k} p_{\hat{k},n}^{ib}$ and $\hat{i}$ denotes user who has the maximum priority at the n-th subchannel with reuse factor k in BS b.

The matrix $\mathbf{Q}_{best}^b$ is determined as follows:

$$\mathbf{Q}_{best}^b = \left(e_{k^*,1}^{\hat{i}(k^*,n,b)b}, e_{k^*,2}^{\hat{i}(k^*,n,b)b}, \cdots, e_{k^*,n}^{\hat{i}(k^*,n,b)b} \right), \tag{11}$$

where $k^*(n,b) = \arg\max_k e_{k,n}^{\hat{i}b}$ and k^* denotes reuse factor corresponding to the maximum value among spectral efficiencies of n-th subchannel in BS b. $k^*(n,b)$, $\mathbf{Q}_{best}^b$, and $\mathbf{Q}^b$ evaluated at each BS are sent to RNC.

3) *Cell coordination*: RNC executes cell coordination as follows.

Step 1. *Reuse factor Determination for each subchannel*: The number of reuse factors requested from all BS calculations in each subchannel are counted. A nominal reuse factor in each subchannel is determined one that receives the largest request from all BSs in order to use efficiently available system bandwidth. For example, if the requested number of reuse factors of 1, 3, and 7 at a certain subchannel gathered from all BSs are 9, 9, and 1, respectively, the nominal reuse factor in the subchannel is determined to be 3. Once the nominal reuse factor is fixed to be k in a subchannel, then the nominal spectral efficiency is determined as the largest one among the spectral efficiencies of those BS having requested reuse factor of k.

Step 2. *Band partitioning for reuse factor seven*: Different band partitioning methods can exist and one of them was implemented below. We need to compare the performance and the complexity with respect to different band partitioning ways from now on.

The proposed schemes determine the band of frequency reuse factors of k by moving subband windows covering 7 consecutive subchannels over the entire band. In each move, the number of times a reuse factor of 7 occurred is counted and the spectral efficiencies of subchannels exhibiting a reuse factor of 7 are summed to represent the spectral efficiency of the subband. Windows having more than four subchannels of reuse factor 7 are assigned as candidate subbands of reuse factor seven. Subsequently, subband window of size seven is moved right by one subchannel and the procedure is repeated until the subband window of size seven covers all subchannels. In order to determine the subband of reuse factor 7 among the candidates, the sums of spectral efficiencies of subbands are sorted by descending order. If two subbands are overlapped, the subband having the smaller sum is removed.

Step 3. *Band partitioning for reuse factor three*: Step 2 is repeated for subbands having a reuse factor of 3. In this instance, subband windows having more than two subchannels of reuse factor of 3 become candidates for the category.

Step 4. *Band partitioning for reuse factor one*: After steps 2 and 3 are conducted for reuse factors 7 and 3, all remaining subchannels that are not yet determined are assigned a reuse factor equal to 1. k_n, which represents the assigned reuse factors for each subchannel, is thereby generated in this step.

Step 5. *BS determination for each subchannel*: For subbands of reuse factor 7, RNC allocates each subchannel to the BS having the largest spectral efficiencies among seven BSs. If two or more subchannels are assigned to the same BS, RNC allows BS to select only one subchannel having the largest spectral efficiency and repeats subchannel allocation for the those subchannels that have yet to be assigned to BS. The identical method is used to allocate subchannels of reuse factor 3 to each BS. The matrix $\mathbf{B}$, indicating which BS uses a certain subchannel, is determined as follows:

$$\mathbf{B} = (b_0, b_1, \cdots, 0, \cdots, b_n)\,, \tag{12}$$

where b_n is the BS index of the n-th subchannel and $b_n = 0$ denotes that the reuse factor of the n-th subchannel is 1.

Step 6. *Subchannel allocation to BS*: RNC transmits k_n and the matrix $\mathbf{B}$ to BSs.

4) *Allocating subchannel to MS*: Each BS receives the information about the subchannels to be used and the reuse factors assigned. BS allocates each subchannel to user with highest priority during one downlink frame using the matrixes $\mathbf{Q}^b$, $\mathbf{B}$, and the value for k_n.

5 Simulation Results

5.1 Simulation Environments

Table 1 shows parameters of IEEE 802.16e-based TDD-OFDMA system. The MCS level [13][14] is reported to users according to SINR sensitivity thresholds and the delay of one frame is assumed in MCS feedback. The existence of 37 cells having a 1km cell radius is assumed. The required data rate is assigned to be the same for all users. MSs are distributed uniformly in BSs and the number of MSs per cell is assumed from 2 to 15. The path loss model is assumed to be $PL = 129.427 + 37.6 * \log_{10}(d_{km})$ [9][10] and the standard deviation of log-normal shadowing is 10 dB. Short-term channel gains are assumed to be Rayleigh fading with a Doppler frequency of 6.4Hz and the tapped-delay-line multipath models from ITU-R were used [11]. The BS transmitted power and antenna gains were set to values of 20 W and 14 dBi, respectively. The thermal noise density was assumed to be -174 dBm/Hz and the maximum C/I value was limited to 30 dB. In all performance figures, the notations of sp and nsp denote the spectral efficiency and the spectral efficiency normalized by the average throughput.

Table 1. System parameters [12]

Parameters	Value
Carrier Frequency	2.3 GHz
Channel Bandwidth	10 MHz
Number of subcarriers	1,702 of 2,048
Number of traffic subcarriers	1,536
Subcarrier spacing	5.57617 kHz
Number of subchannels	32
Number of subcarriers	48
Frame length	5.0 msec
Number of DL symbols	18
OFDMA symbol time	190.543 μsec
Guard interval	11.208 μsec

5.2 Cell Throughput Performance

The cell throughput of the static and dynamic cell coordination schemes for the various numbers of users in frequency flat fading are shown in Fig. 2 and 3. Cell throughput using SSAS [8] decreases as the number of users increases to greater than five because of the increased likelihood of more users requesting more subchannels of reuse factor 7. When the target data rate is 384kbps and the number of users becomes larger, the cell throughput of greedy cell coordination scheme 2 outperforms SSAS by a maximum of 66%. In the case of 64kbps, the greedy cell coordination scheme 3 achieves an average of 3.6 times greater cell throughput compared to SSAS. The performance of greedy scheme 3 is

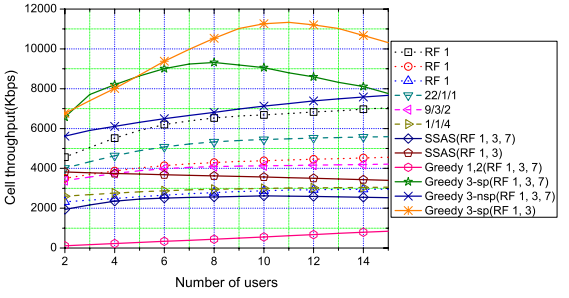


Fig. 2. Cell throughput comparison for the static approach, SSAS, and the schemes proposed for a data rate of 64kbps in frequency flat fading

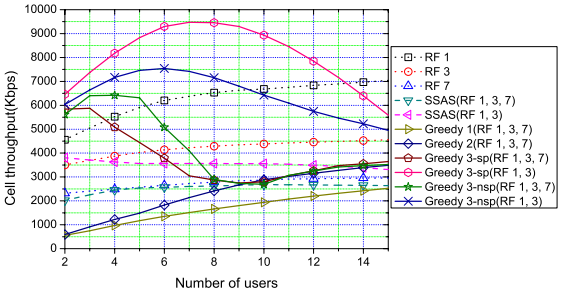


Fig. 3. Cell throughput comparison of SSAS and the schemes proposed for a required data rate of 384kbps in frequency flat fading

degraded as the number of users increases since fewer users are allocated the required throughput when the required data rate of users is 384kbps. The cell throughput of greedy scheme 3 using reuse factors equal to 1 and 3 is decreased as compared to applying the scheme using reuse factors 1, 3, and 7.

The cell throughput comparison of various cell coordination systems including no coordination and dynamic coordination within a range of the number of users in frequency selective fading is illustrated in Fig. 4. DMCC demonstrates the best cell throughput because it allocates subchannels to users having good channel condition. The cell throughput of DMCC analysis using all reuse factors of 1, 3, and 7 is about 2.6 times greater than that for the scheme using a reuse factor of only 1. DPFCC exhibit relatively low throughput as compared to DMCC because the fairness among users is considered. Nevertheless, the cell throughput is similar to that of the case using the single reuse factor of 3 as the number of users increases. Also, the DPFCC using reuse factor 1 and 3 approaches to the cell throughput of the case of single reuse factor 1. DMCC and DPFCC calculations using reuse factor values of 1 and 3 demonstrate 24% and 57% more

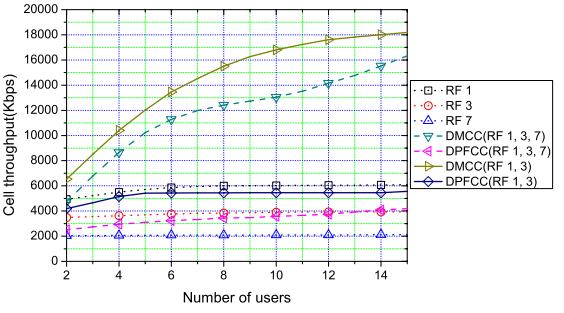


Fig. 4. Cell throughput comparison of schemes proposed using reuse factor values of 1, 3 and 7 or reuse factor values of 1 and 3 in frequency selective fading

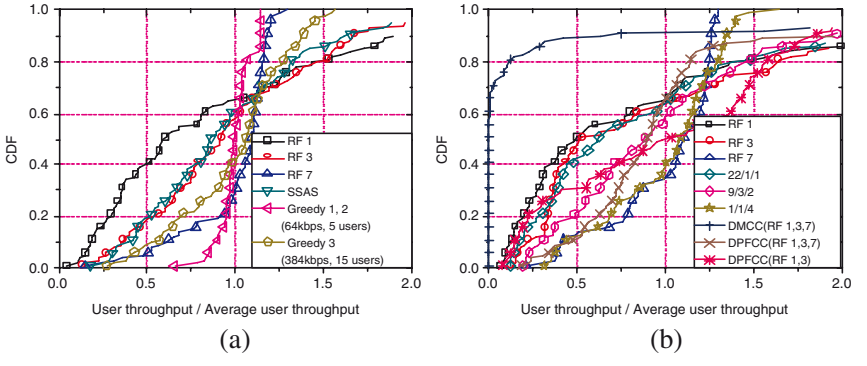


Fig. 5. (a) Fairness comparison of SSAS and the proposed schemes in flat fading; (b) Fairness comparison of proposed schemes in selective fading

cell throughput, respectively, compared to calculations using all reuse factor values of 1, 3 and 7 because the subchannel with reuse factor 7 used one seventh of the total subchannels available.

5.3 Fairness Performance

The relative fairness of SSAS and the schemes proposed in this research were compared for frequency flat fading, given that the numbers of users are 5 and 15 and the required data rates of users are 64kbps and 384kbps, respectively in Fig. 5(a). The fairness of SSAS is similar to the case using the single reuse factor equal to 3 and is independent of the number of users and the required data rate of users. When the required data rate of users is 64kbps, the greedy scheme 1 and 2 demonstrate better fairness than the case using a reuse factor of 7. As the required data rate for 15 users was 384kbps, the fairness of greedy scheme 3 approach to the case of 64kbps using greedy schemes 1 and 2 because there are hardly the remaining subchannels.

The fairness comparison of the proposed schemes assuming 15 users in frequency selective fading was also assessed in Fig. 5(b). The fairness values of (22/1/1) and (1/1/4) approach to that for single reuse factors equal to 1 and 3, respectively. DMCC demonstrate the worst fairness because it allocates subchannels to the users having the best channel quality. By using DMCC, 65% of users are not served while the fairness is degraded. The fairness assessment of DPFCC using all reuse factors of 1, 3, and 7 achieve better performance than that of (9/3/2). The fairness level of DPFCC using reuse factors 1 and 3 is poorer than that of DPFCC using reuse factors of 1, 3, and 7. In flat and selective fading environment, it is observed that most of cell coordination schemes could offer data service to users in the cell boundary by improving their SINRs using large reuse factors.

6 Concluding Remarks

Two different dynamic cell coordination schemes considering jointly adaptive modulation and variable frequency reuse were proposed to allocate subcarrier efficiently in the channel condition aware OFDMA downlink multicell system. The performance was evaluated in frequency flat and selective fading. The proposed system dynamically allows RNC to apply different reuse factors on each subchannel and scheduling in consideration of channel and interference conditions of individual users so as to increase the system throughput and guarantee QoS of each user. In frequency flat fading, for the required data rate of 64kbps, it was demonstrated that greedy scheme 3 achieved on average a 3.6 times higher cell throughput as compared to SSAS and that greedy schemes 1 and 2 produced the best performance of fairness. At the required data rate of 384kbps, the cell throughput of greedy scheme 3 was, at the maximum, 3 times higher than that of SSAS. Greedy scheme 3 approached to the case of 64kbps using greedy schemes 1 and 2. In frequency selective fading, the cell throughput of DMCC was, at the maximum, 2.6 times higher than that of the case using a reuse factor of 1, and the fairness of DPFCC approached that when the reuse factor equal to 7 was applied.

Acknowledgment

This work was supported by the Korea Research Foundation Grant (KRF-2004-013-D00060).

References

1. Kivanc D., Li G., Liu H.: Computationally Efficient Bandwidth Allocation and Power Control for OFDMA. IEEE Transsaction on Wireless Communications, Vol. 2. IEEE. (2003) 1150-1158.
2. Tse D.: Multiuser diversity in wireless networks. Wireless communication seminar, (2001).

3. Wong C. Y., Cheng R. S.: Multiuser OFDM with Adaptive Subcarrier, Bit, and Power Allocation. IEEE Journal on Selected Areas in Communication, Vol. 17. IEEE. (1999) 1747-1758.
4. Kivanc D., Liu H.: Subcarrier Allocation and Power Control for OFDMA. Signals, Systems and Computers, Conference Record of the Thirty-Fourth Asilomar Conference on, Vol. 1. (2000) 147-151.
5. Suzuki M., Bohnke R., Sakoda K.: Band division multiple access (BDMA) system: A novel approach for next generation mobile telecommunication system, based on OFDM and SFH-TDMA. IEEE Vehicular Technology Conference (VTC 1998).
6. Zander J., Frodigh M.: Capacity allocation and channel assignment in cellular radio systems using reuse partitioning. Electronics Letters, Vol. 28. (1992) 438-440.
7. Blair P., Polyzos G. C., Zorzi M.: Plane Cover Multiple Access: A New Approach to Maximizing Cellular System Capacity. IEEE Journal on Selected Areas in Communication, Vol. 19. IEEE. (2001) 2131-2141.
8. Kim H., Han Y., Koo J.: Optimal Subchannel Allocation Scheme in Multicell OFDMA Systems, IEEE Vehicular Technology Conference (VTC 2004) 1821-1825.
9. Recommendation ITU-R M.1225, Guideline for Evaluation of Radio Transmission Technologies for IMT-2000, (1997).
10. TTAR-0016, Evaluation Criteria of Radio Access Technology for 2.3GHz Portable Internet, Telecommunications Technology Association (TTA), (2004).
11. 3GPP R1-030042, Update of OFDM SI simulation methodology. (2003).
12. http://www.ieee802.org/16/tge
13. IEEE C802.16d-03/78r1, Coverage/Capacity simulation for OFDMA PHY in with ITU-T channel model, (2003).
14. IEEE C802.16d-04/50r3, OFDMA PHY Enhancements for better mobility performance, (2004).

Comparative Analysis Among Different Monitoring Functions in a Bandwidth Renegotiation Scheme for Packet Switched Cellular Networks

Hermes Irineu Del Monego[1], Luiz Nacamura Junior[1], Richard Demo Souza[1], Anelise Munaretto Fonseca[1], and Marcelo Eduardo Pellenz[2]

[1] LASD – CPGEI – UTFPR – Curitiba – PR, CEP 80230-901, Brazil
{hermes, richard, nacamura, anelise}@cpgei.cefetpr.br
[2] PPGIA – PUC-PR – Curitiba – PR, CEP 80215-901, Brazil
marcelo@ppgia.pucpr.br

Abstract. In this paper we present a comparison among three different monitoring functions to be used in a dynamic bandwidth renegotiation scheme. These functions aim at detecting the amount of unused resources in the network, which can be allocated to low priority data flows. These applications are not delay-sensitive and can be admitted by the call admission control with a bandwidth smaller than the nominal one. Simulation results comparing the performance of the three monitoring functions are presented, as well as an overhead analysis. Finally, we discuss the performance/complexity trade-off considering the three functions and determine the most viable one.

Keywords: Resource Management, QoS in Mobile and Wireless Networks, Packet Switched Cellular Networks, Bandwidth Renegotiation.

1 Introduction

Recently, there has been a lot of research towards the Quality of Service (QoS) provision for packet switched cellular networks, as GPRS, EDGE and UMTS [1-3]. Such studies have been carried out privileging real-time traffic, where the delay sensibility is more relevant [4].

In [1] the authors present a bandwidth renegotiation scheme for post-admitted calls. The basic idea is to explore any unused resources in the network, allocating them to applications with lower priority which have been admitted with a low bandwidth. The renegotiation scheme in [1] considers two methods for detecting the unused resources: i) by the effective average bandwidth utilized by the high priority flows; ii) by the termination of the data flow of a given application. Hereon these methods for detecting the unused resources are called monitoring functions.

However, in [1] the two monitoring functions are applied at the same time, and the contribution of each function in the overall system performance is not clear. Moreover, in [1] the authors do not draw an analysis of the amount of overhead produced by the renegotiation scheme. Each access to the monitoring functions generates some traffic in the control channels, besides a particular computational load associated with each function.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 76 – 87, 2006.

In this paper we present an effective comparison among three different monitoring functions that can be used in the proposed bandwidth renegotiation scheme. The three functions differ in the methods considered for the evaluation of the unused resources: i) by the average bandwidth; ii) by the flow termination; iii) by the combination of both average bandwidth and flow termination. The comparison is made both in terms of global performance, where the metric is the amount of bandwidth allocated to low priority data flows, as in terms of overhead, where the metric is the number of calls to the monitoring functions during the system operation. Then, we discuss the trade-offs between performance and complexity for the three functions and analyze their practical viability.

This paper is organized as follows. In Section 2 the architecture of a GSM/GPRS/EDGE network, which is used as reference in this work, is presented. The renegotiation mechanism and the three monitoring functions are presented in Section 3. The implementation and simulation of two hypothetic scenarios, which demonstrate the functionality of the proposed functions, are presented in Sections 4 and 5, while in Section 6 we draw a comparative analysis among the three strategies. Finally, in Section 7 we conclude the paper.

2 Bandwidth Renegotiation in a GPRS/EDGE Network

The renegotiation mechanism can be implemented in a GPRS/EDGE network through the incorporation of a renegotiation function in the call management system. This module collects the information regarding the bandwidth utilization in the MAC layer, and renegotiates with the SGSN the modifications in the bandwidth allocated to the active flows. The information regarding each flow is collected by a monitoring function. The collected data is then transferred to the renegotiation function. The architecture of a GPRS/EDGE network incorporating the renegotiation modules is presented in Fig. 1.

3 The Renegotiation Scheme

The system for call admission control (CAC) used in this work was proposed in [5], and associates different priorities to different QoS classes. *Conversational* class applications are associated to a maximum priority (priority 1), and are admitted only if there is enough bandwidth at the request time. Priority 2 (intermediate) is given to *streaming* class applications, where again the requests are admitted only if there are enough resources. Priority 3 (the lowest priority within the mechanism) is associated with the *interactive* and *background* class applications. Priority 3 applications can be admitted with less bandwidth than the requested one. In the CAC defined in [5], the allocated bandwidth is kept constant even if more bandwidth becomes available in the system before the end of the admitted low priority application transmission. Another limitation of this CAC mechanism is that, if applications with priorities 1 and 2 do not effectively use the whole bandwidth allocated to them at call admission time, these unused resources can not be transferred to lower priority applications.

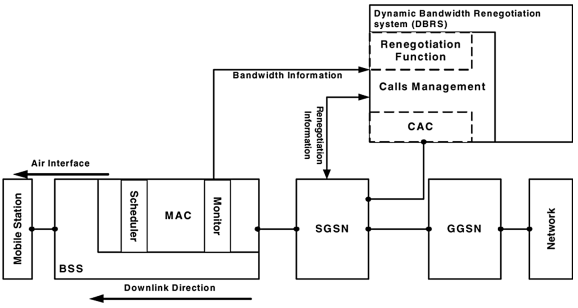


Fig. 1. Block diagram of a packet switched cellular system with the insertion of the renegotiation scheme

The renegotiation scheme proposed in [1] has the objective of allowing that priority 3 applications use, temporarily, more bandwidth than the one allocated to them by the CAC. This possibility can be due to unused resources by applications with priorities 1 and 2, or due to the termination of another application of any priority. If an application with priority 1 or 2 arrives, and the system does not have enough bandwidth for admitting that call, the renegotiation mechanism can reduce the bandwidth being used by priority 3 applications to the value originally allocated to them by the CAC. This guarantees that applications with higher priorities will not be harmed by the renegotiation mechanism.

Therefore, the renegotiation mechanism consists in increasing the bandwidth of priority 3 applications when there are unused resources within the system, and to restore (decrease) the bandwidth of these applications at the arrival of an application with priorities 1 or 2. In the latter case, it occurs what we have called "renegotiation by priority demand", while the former case, we have called "renegotiation by the average bandwidth and/or flow termination".

As mentioned before, the information regarding the bandwidth being effectively by the active data flows is collected by the monitoring functions. In this paper we consider the used of three different monitoring functions, which consider the average bandwidth used by the active data flows, the bandwidth released by any flow termination, or both.

3.1 The Average Bandwidth

The renegotiation by the average of the utilized bandwidth consists in calculating the amount of unused bandwidth by the admitted calls. If the effectively used bandwidth is smaller than the admitted one, then the renegotiation starts and the unused resources are allocated to lower priority flows. Samples of the bandwidth utilized by the flows within the system are measured by the monitoring function. The quantity of bytes within each flow are summed during one time interval Δt. For each Δt, we obtain a partial average by dividing the number of transmitted bytes by the period Δt[1].

[1] Strictly speaking, we calculate the average data rates, not the bandwidth. However, in this paper we use the terms bandwidth and data rate interchangeably.

The n-th sample of the average used bandwidth can be calculated as:

$$\overline{Bm_n} = \frac{\sum_{p=1}^{P} Psize_{p_n}}{\Delta t_n}, \tag{1}$$

where, $Psize_p$ is the packet size, Δt is the duration of each sample and P is the number of packets. Thus, in order to obtain the average used bandwidth, $\overline{Bm_t}$; we have:

$$\overline{Bm_t} = \frac{\overline{Bm_1} + \overline{Bm_2} + \overline{Bm_3} + \cdots + \overline{Bm_N}}{N}, \tag{2}$$

where N is the number of samples.

Following the normal distribution, we can say that the average used bandwidth, $\overline{Bm_t}$, becomes reliable when the number of samples is larger than 30, $N > 30$ [6]. The standard deviation σ_b of the samples can be determined through the variance:

$$\sigma_b^2 = \frac{\sum_{n=1}^{N} \left(\overline{Bm_n} - \overline{Bm_t}\right)^2}{N-1}. \tag{3}$$

As the standard deviation is calculated from the samples only and not from the whole population, we use the student's t-distribution [6] to approximate the values of the total used bandwidth within the interval:

$$\left[\overline{Bm_t} - t_{N-1}\frac{\sigma_p}{\sqrt{N}}; \overline{Bm_t} + t_{N-1}\frac{\sigma_p}{\sqrt{N}}\right], \tag{4}$$

where, t_{N-1} is the constant of student for N-1 samples.

Then, as a conservative estimate, we use the upper limit of the above interval as the measured total used bandwidth Bt_m. In this case, we can determine the difference between the bandwidth admitted by the CAC (B_{wCac}) and the estimate of the total used bandwidth Bt_m:

$$B_\Delta = B_{wCac} - B_{tm} \tag{5}$$

where B_Δ corresponds to the unused bandwidth that can be renegotiated.

3.2 Flow Termination

The renegotiation by flow termination consists in allocating more bandwidth for a low priority flow when another flow ends. The released bandwidth can be reallocated to another flow whose allocated bandwidth is smaller than the one requested to the CAC.

Fig. 2-(a) shows two different flows in a system without renegotiation. In this case, even though some bandwidth is available in the system after the termination of flow

A, the bandwidth allocated to flow **B** does not change. Fig. 2-(b) shows what happens in case of renegotiation by flow termination. Note that when flow A ends at time instant t_3, the renegotiation function increases the bandwidth allocated to flow B up to the requested amount.

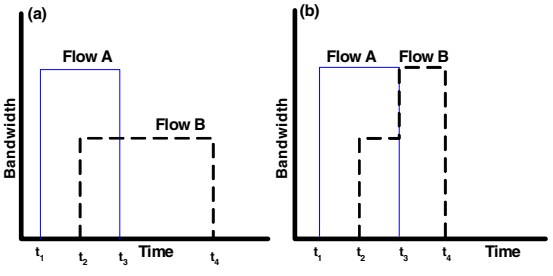


Fig. 2. (a) Behavior of two different flows without (a) and with (b) renegotiation

4 Simulation Parameters

The renegotiation scheme was implemented in the NS-2 [7]. Two hypothetical scenarios were investigated with the objective of verifying the behavior of the three proposed monitoring functions. In the first scenario, we have generated data flows of ftp, voice, telnet and e-mail. The second scenario, more complex, contains data flows of video, music, e-mail, telnet and www. Table 1 presents the QoS classes associated with each application, in accordance with [4].

Table 1. QoS classes associated with each application under consideration

QoS Class	Priority	Application
Conversational	1	telnet, voice
Streaming	2	music, video
Interactive	3	ftp, www
Background	3	e-mail

In the simulations, we have used the data flows available within NS-2 [7] for the case of telnet, ftp, music and voice applications. For the case of video and www applications we utilized the traces available in [8] and [9], respectively. For the e-mail we utilized the traces available in [11] and [13]. The average duration of each application was simulated according to [4], [10], [11], [12] and [14]. The number N of samples varied between 30 and 40 in order to satisfy the confidence constraints presented in Section 3.1-A. Table 2 presents a summary of the parameters used in the simulations.

Moreover, it is necessary to define the amount of bandwidth requested to the CAC by each application. Tables 3 and 4 present this amount for each application to be considered in the two scenarios that are explored in the next Section, respecting the

limits established in Table 2. For instance, an ftp call requests a bandwidth of 85 kbps. As ftp is a priority 3 application, the allocated bandwidth can be smaller than this amount. In case of applications with priorities 1 or 2, such as the telnet that requires transmission rate of 1.1 kbps, the call can be admitted only if the full requested bandwidth is available.

Table 2. Simulation Parameters

Application	Nominal Bandwidth (Kbps)	Average Call Duration (min-max)	Inter-Arrival Time
Telnet	1.11	3 minutes (30s–max)	Exponential
Voice	4-25	3 minutes (60s–max)	Constant
Music	5-128	3 minutes (60s-max)	Constant
Video	20-384	6 minutes (100s–max)	24 frames/s
Ftp	< 384	2 minutes (30s-max)	Exponential
E-mail	4.4	30 seconds (10s–120s)	Exponential
www	-		Exponential

Table 3. Required bandwidth for each application in scenario 1

	Applications			
	telnet	**voice**	**ftp**	**e-mail**
Required Bandwidth (kbps)	1.11	21.3	85	4.4

Table 4. Required bandwidth for each application in scenario 2

	Applications				
	e-mail	**music**	**telnet**	**www**	**video**
Required Bandwidth (kbps)	4.4	21.3	1.11	65	85

5 Numerical Results

In this section we present numerical results in two hypothetical scenarios, for the throughput performance of a packet switched cellular network in four different cases: i) without bandwidth renegotiation; ii) with bandwidth renegotiation based in the average bandwidth monitoring function; iii) with bandwidth renegotiation based in the flow termination monitoring function; iv) with bandwidth renegotiation where the monitoring function takes into account both average bandwidth and flow termination.

5.1 System Without Bandwidth Renegotiation

Fig. 3(a) shows the behavior of data flows for the scenario 1 applications (according to Table 3) where there is no bandwidth renegotiation and the allocated bandwidth is

determined by the CAC only. From the figure we can see that, even though applications ftp1 and ftp2 required the same amount of bandwidth to the CAC (85 kbps), ftp2 is allocated only a fraction of that (32 kbps). This is due to the fact that there are not enough resources available in the network at the call arrival.

The telnet and voice flows, which have high priority, were admitted with the nominal bandwidth, respectively 1.11 and 21.3 kbps. The e-mail flow, even though of low priority, was admitted with the required bandwidth of 4.4 kbps since, at the call arrival, there were enough resources in the network (the voice flow terminated at time instant 120s). Note that, during the whole simulation the bandwidth allocated to each application is kept constant.

Fig. 3(b) shows similar results but considering scenario 2 (Table 4), which is compose by video, music, www, telnet and e-mail. The www data flow is admitted with the resources available at that moment (8 kbps only), which is kept until the end of the www flow, even though after the video termination there are a good amount of available resources in the network.

5.2 System with Renegotiation: Average Bandwidth

Fig. 4(a) presents the performance results for the first scenario, considering that the renegotiation mechanism is implemented with the average bandwidth monitoring function only. In this case the ftp2 flow is admitted with 33 kbps, at stage (a) in the plot. Soon, the value is increased to 34 kbps at stage (b). This small increase in the allocated bandwidth, compared to the case without renegotiation, is due to some available resources detected by the average bandwidth monitoring function.

Fig. 4(b) considers the applications for the second scenario. In this case the renegotiation occurs in two stages. At stage (a) the www flow is allocated 12 kbps, an increase of 4 kbps when compared with the case without renegotiation. At stage (b) the amount was increased to 19 kbps. Again, this difference compared to the case without renegotiation is due to the use of a function that monitors the bandwidth being effectively used by the current data flows.

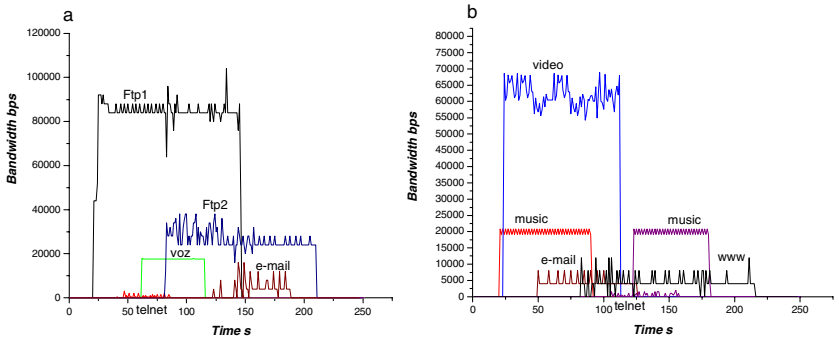


Fig. 3. (a) Combination of e-mail, ftp, voice, and telnet without renegotiation, (b) Combination of e-mail, music, telnet, video and www without renegotiation

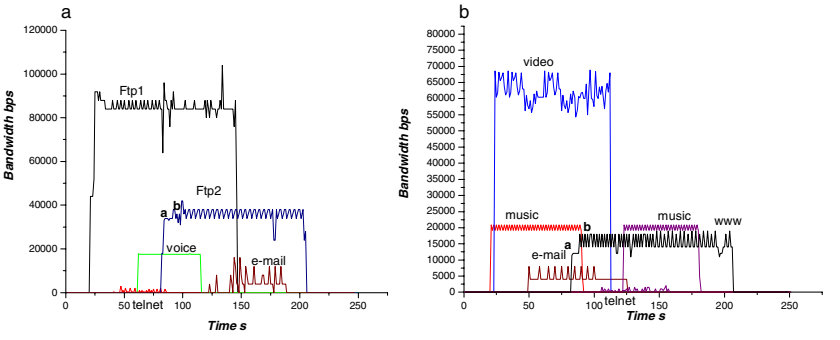


Fig. 4. (a) Bandwidth renegotiation with an average bandwidth monitoring function for an ftp data flow, (b) Bandwidth renegotiation with an average bandwidth monitoring function for a www data flow

5.3 System with Renegotiation: Flow Termination

Here we consider a system with bandwidth renegotiation, but the monitoring function is based only on the flow termination. Fig. 5(a) shows the performance results for the first scenario. The ftp2 flow is admitted with 33 kbps, at stage (a), and at stage (b) the bandwidth is increased to 34 kbps due to the termination of the telnet application. Renegotiation happens again at stage (c), where now the ftp2 flow is allocated 46 kbps. Finally, at stage (d) the ftp1 flow terminates and then the bandwidth allocated to the ftp2 application is increased even more, now to 85 kbps what is 100% of the nominal bandwidth.

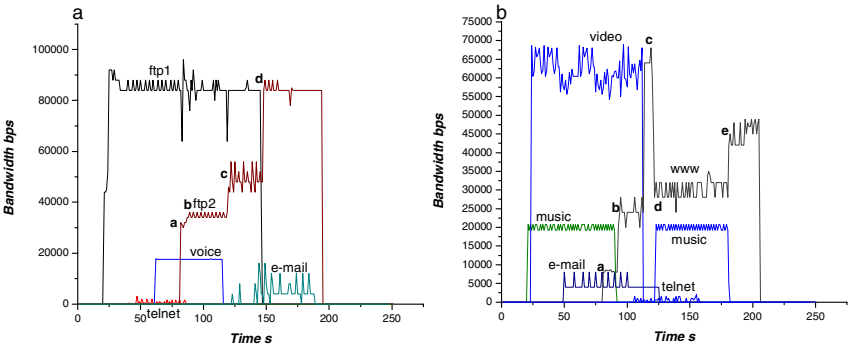


Fig. 5. (a) Bandwidth renegotiation based on flow termination for an ftp data flow, (b) Bandwidth renegotiation based on flow termination for a www data flow

Fig. 5(b) considers the second scenario. Note that the www flow is admitted with only 8 kbps. The first renegotiation occurs at stage (b), where the bandwidth is increased to 24 kbps. The www flow reaches 100% of the nominal bandwidth at stage (c). Then, happens what we call renegotiation by priority demand, and the bandwidth

allocated to the www flow has to be decreased to 28 kbps at stage (d). Finally, at stage (e), the bandwidth is increased to 42 kbps due to the termination of the music flow.

5.4 System with Renegotiation: Average Bandwidth and Flow Termination

Here we consider that the monitoring function takes into account both the average bandwidth being effectively used by the high priority flows and the possible bandwidth released by any flow termination. Fig. 6(a) shows results considering scenario 1. Note that the ftp2 application is admitted with a smaller bandwidth than the requested one. However, the bandwidth is successively increased until it reaches the nominal bandwidth at stage (d). Note that renegotiation is due both to the average bandwidth, as in stage (b), and to flow termination, as in stage (d).

Fig. 6(b) considers the second scenario, where the focus is the www flow. Note that at stage (f) happens a renegotiation by priority demand, while in stage (g) part of the bandwidth is reallocated due to the termination of the music flow. Again, renegotiations due to average bandwidth, as in stage (b), and to flow termination, as in stage (g), can be seen.

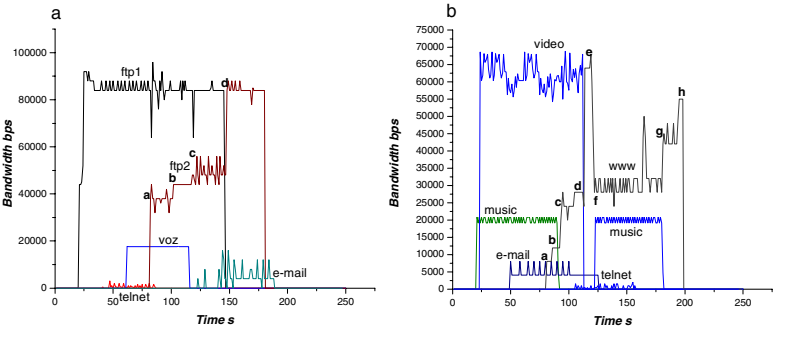


Fig. 6. (a) Bandwidth renegotiation based on flow termination and average bandwidth for an ftp data flow, (b) Bandwidth renegotiation based on flow termination and average bandwidth for a www data flow

6 Comparative Analysis

In this section we draw a comparative analysis, based on performance and overhead, among the three different monitoring functions investigated in the previous section.

6.1 Global Performance

For the sake of performance comparison we introduce an index called “global performance” (*Gp*). This metric is defined as the average of the increase in the allocated bandwidth when compared with the case where there is no bandwidth renegotiation. The average is calculated based on the sampling points represented by the stages marked in Figs. 4–6. Thus, *Gp* can be defined as:

$$Gp = \sum Per / Nc \tag{6}$$

where *Per* is the percentage increase in the allocated bandwidth with respect to the bandwidth that would be allocated without renegotiation, and *Nc* is the number of stages in each case [2].

Fig. 7(a) shows the *Gp* index for the first scenario (where the focus is ftp flow) considering the three different monitoring functions: i) average bandwidth; ii) flow termination; iii) average bandwidth and flow termination. In the case of average bandwidth, *Gp* equals only 4.73%, which means that the performance increase was very small compared to the case without renegotiation. In the case of flow termination *Gp* was much larger, of 54.6%, reaching 74.05% for the case of both average bandwidth and flow termination. Note that the *Gp* index for the case of flow termination is of the order of 10 times the index for the case of average bandwidth, and it is relatively close to the index for the case of both methods.

Fig. 7(b) shows the same comparison but for the second scenario (where the focus is the www flow). The *Gp* index was of 93% for the case of average bandwidth, while for the case of flow termination as of 353.2% and for the case of both methods it was of 358,7 %. These large values for the *Gp* index are due to the fact the bandwidth originally allocated by the CAC was very small. And in this scenario the values for the *Gp* index are very close for the cases of flow termination and both flow termination and average bandwidth. For the case of average bandwidth, the *Gp* index is considerably smaller than for the other two cases.

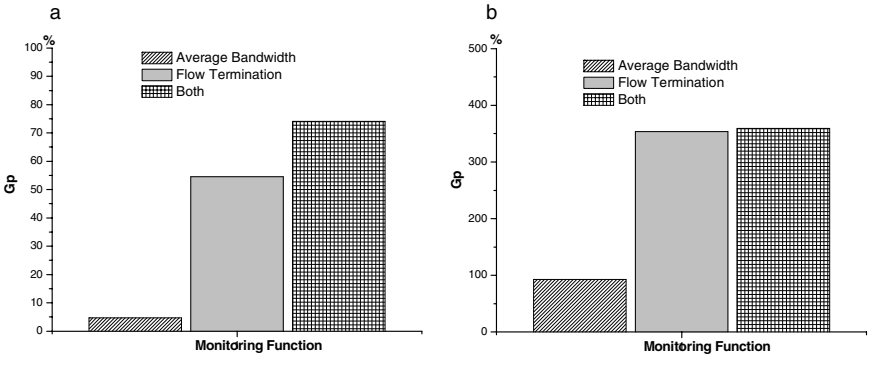


Fig. 7. (a) Global performance index for scenario 1, (b) Global performance index for scenario 2

From the above results, we can see that most of the performance increase comes from the allocation of bandwidth released by any flow termination, but the best performance is always achieved by the case of the monitoring function that takes into account both the average bandwidth and flow termination. However, in order to draw some conclusions on possible trade-offs, it is necessary to investigate the overhead generated by the proposed monitoring functions.

[2] The stages were inserted in Figs 4-6 in the time instants where some relevant bandwidth renegotiation happened. This is the reason why the number of stages differ for each monitoring function.

6.2 Overhead Analysis

The overhead generated by the monitoring functions can be estimated by counting the number of times that each function is called during the period that a given flow is active. For the first scenario, where the focus is the ftp flow, the monitoring function is called a total of 20 times for the case of both average bandwidth and flow termination. In the case of the average bandwidth, the monitoring function is called 17 times. For the case of the termination flow monitoring function, the number of calls is of only 3 times.

Fig. 8(a) shows a bar plot comparing the number of times that each function is called for the first scenario, while Fig. 8(b) presents similar results but for the second scenario. For both scenarios we can see that the number of times that the monitoring function is called is very similar for the case of average bandwidth and for the case of average bandwidth and flow termination. However, for the case of the flow termination, the number of function calls is very small. Thus, the amount of overhead generated by the average bandwidth monitoring function is much larger than for the flow termination monitoring function.

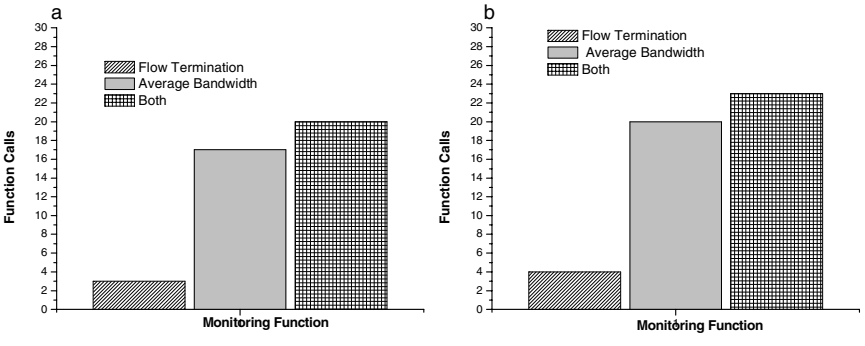


Fig. 8. (a) Number of monitoring function calls for the first scenario, (b) Number of monitoring function calls for the second scenario

Analyzing the results presented in Figs. 7 and 8, we can say that most of the performance gain comes from the flow termination monitoring function. Also, most of the overhead is produced by the average bandwidth monitoring function. Thus, in terms of performance/complexity trade-off, the monitoring function that considers only flow termination is a much better choice than the monitoring functions that consider either the average bandwidth or both the average bandwidth and the flow termination. Even though the performance results for the case of a monitoring function considering both the average bandwidth and the flow termination (as considered in [1]) are superior, due to high overhead of the monitoring of the average bandwidth, it is practical application seems unfeasible. On the other hand, the monitoring function considering only the flow termination presents very good performance results while introducing low overhead in the network. Thus, it is application in a real-time bandwidth renegotiation scheme seems feasible.

7 Conclusions

In this paper we presented a comparative analysis of three different monitoring functions that can be used in a bandwidth renegotiation system implemented in a GPRS/EDGE network. The bandwidth renegotiation mechanism explores any unused resources in the network, allocating them to lower priority flows.

The renegotiation scheme was implemented in the NS-2. Two hypothetic scenarios were considered. The performance of the renegotiation scheme using each of the three different monitoring functions was compared relatively to the case where there is no bandwidth renegotiation. Also, we investigated the amount of overhead that each monitoring function would introduce in the network. The final conclusion is that the monitoring function that considers only the flow termination is the one that presents the best performance/complexity trade-off among the three functions considered in this paper.

References

1. Del Monego, H.I., Bodanese, E.L., Junior, L.N., Souza, R.D.: A Dynamic Resource Allocation Scheme to Providing QoS in Packet-Switched Cellular Networks. Lecture Notes in Computer Science, Vol. 3744. Springer-Verlag GmbH, Montreal (2005) 117-126
2. Halonen, T., Romero, J., Meleto, J.: GSM, GPRS, and EDGE Performance Evolution Towards 3G/UMTS. John Wiley & Sons, 2nd Edition (2003)
3. 3. Liang, X., Xuemin, S., Mark, J.W.: Dynamic Bandwidth Allocation With Fair Scheduling for Wcdma Systems. In IEEE Personal Communications, Vol. 9, n. 2, (2002) 26 – 32
4. 3GPP TS 23.107.: UMTS Universal Mobile Telecommunications System, Quality of Service. Vol. 5.7.0 www.etsi.org (2003) 1-41
5. Kochem, A.C.B. and Bodanese, E.L.: A quality of service management scheme over GPRS. In: IEEE SoutheastCon (2003) 74–80
6. Levine, D.M., Berenson, M.L., Stephan. D.: Statistics for Managers using Microsoft Excel. Prentice Hall Inc. 2nd Ed (1999)
7. NS-2.: Documentation. UC Berkeley. www.isi.edu/nsnam/ns/ns-documentation.html (2004)
8. Trace.: Trace Files. http://trace.eas.asu.edu/TRACE/ltvt.htm (2004)
9. Nasa.: Traffic Archive. http://ita.ee.lbl.gov/html/contrib/ NASA-http.html (2004)
10. Oliveira, C., Kim, J.B., Suda, T.: An adaptive bandwidth reservation scheme for high speed multimedia wireless networks. In: IEEE Journal on Selected Areas in Communications. Vol. 16, n. 6 (1998) 858-874
11. Staehle D., et al.: Source Traffic Modeling of Wireless Applications. www3.informatik. uni-wuerzburg.de /TR/tr261.pdf (2001)
12. IEEE 802.20.: Traffic Model for MBWA System Simulations. www.ieee.org (2003)
13. Pang, Q., Bigloo, A., Leung,V.C.M., et al.: Service Scheduling for General Packet Radio Service Classes. IEEE WNC, Vol. 3 (1999) 1229-1233
14. Staehle D., et al.: QoS of Internet Access with GPRS. Research Report, http://www3.informatik.uni-wuerzburg.de /TR/tr283.pdf (2002)

Load Balancing Approach for Wireless IEEE 802.11 QoS Enhancement

Issam Jabri[1,2], Nicolas Krommenacker[1], Adel Soudani[2], and Thierry Divoux[1]

[1] Centre de Recherche en Automatique de Nancy (CRAN - UMR 7039),
Nancy-University, CNRS, BP239, 54506 Vandoeuvre, France
{issam.jabri, nicolas.krommenacker,
thierry.divoux}@cran.uhp-nancy.fr
[2] Laboratoire Electronique et Micro Electronique (EμE), Faculté des Sciences de Monastir,
5019 Monastir, Tunisie
adel.soudani@issatso.rnu.tn

Abstract. In the few last years, the deployment of IEEE 802.11 WLAN in hotspots environment had becoming a useful solution providing practical and attractive communication characteristics. However the problem of user bandwidth availability arises as one of the most limit of this solution. In fact, the IEEE 802.11 standards do not provide any mechanism of load distribution among different access points (APs). Then an AP can be heavily overloaded leading to station throughput degradation. This paper deals with this problem. It focuses on the presentation of QoS (Quality of Service) management solution for wireless communication system. It, mainly, presents a protocol structure between mobiles and APs. This protocol is intended to provide best resources allocation and efficiency on communication metrics. An SDL description and MSC simulation is provided as a first step in the development of this protocol.

Keywords: Wireless LAN, Load Balancing, QoS Protocol, SDL.

1 Introduction

In the last few years the IEEE 802.11 technology becomes very interesting. One of its popular uses is its cheap hardware infrastructure price promoting to provide practical and efficient Hotspots environment [1]. The research works [1], [2] carried in this context had proved that additional effort is yet required to build up a system with a high service quality. A specification of further interaction in the IEEE 802.11 protocol between APs and mobiles mainly during the call admission stage will help to ensure some QoS parameters such as load distribution and packet losses. A new standard IEEE 802.11e [14] has been defined to ensure quality of service in Wireless LAN.

This paper presents a protocol specification managing the QoS in the context of Hotspots communication environment. The first part presents an overview of the actual quality of service mechanisms for the IEEE 802.11 wireless LAN. The second part focuses on the description of the general hotspots environment architecture. The third part presents the definition of new protocol primitives between the mobile and the access point managing QoS metrics. Then we present the description of this

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 88 – 99, 2006.

protocol with the SDL language (Specification and Description Language) [5] and some MSC (Message Sequence Charts) simulation results of the behaviour of this protocol. We finish by highlighting future contributions in this field.

2 Overview of QoS Mechanisms for IEEE 802.11 Wireless LAN

2.1 QoS Limitations of IEEE 802.11 Wireless LAN

Channel access control, Quality of Service, and data security are the most important functions of a wireless MAC layer. Wireless links have specific characteristics such as large packet delay and jitter, high loss rate, bursts of frame loss and packet reordering. Furthermore, the wireless link characteristics are not constant and vary over time and place [7]. Mobility of users may cause the end-to-end path to change when users are roaming. Users expect to receive the same QoS once changing their point of attachment. This implies that the new path should also support the existing QoS, and problems may arise when the new path cannot support such requirements [7]. The original IEEE 802.11 networks (DCF) are best effort networks and do not support QoS for time critical applications. All stations in a BSS have the same priority to access the channel. There are no differentiation mechanisms to guarantee bandwidth, packet delay or jitter for high priority stations with times-bounded applications or multimedia flows. In [7], authors have make simulations on an ad hoc topology in which stations transmit three types of traffic (audio, video and background traffic) to each other. These simulations clearly shows that there is no throughput or delay differentiation between different flows since only one queue is shared by all the three flows. So, there is no way to guarantee the QoS requirements for high-priority audio and video traffic unless admission control is used.

A PCF mode has been designed to support time-bounded multimedia applications, but it has many problems that lead to poor QoS performances [12], [13]. In this mode wireless resources are wasted since all communications between stations in the same BSS have to go through the Access Point. This mode must be implemented with the DCF mode. Cooperation between Contention Period and Contention Free Period may lead to unpredictable beacon delays [13]: to switch from DCF to PCF, the wireless channel must be idle. The access point is not authorised to stop an established communication to make on the PCF mode and then we have no guarantee on the DCF mode duration. With PCF mode, it is difficult to an access point to define time needed by each polled station to transmit data frames. The transmission time of polled stations is difficult to control since the physical rate can be changed according to the varying channel status.

All these limitations for both DCF and PCF led to a large number of research activities to enhance the performance of 802.11 MAC.

2.2 QoS Mechanisms for IEEE 802.11 Wireless LAN

Most existing QoS mechanism for 802.11 can be classified into three categories [15]:

Service Differentiation. Basically, service differentiation is achieved by two main methods: priority and fair scheduling [16]. While the former binds channel access to different traffic classes by prioritized contention parameters, the latter partitions the channel bandwidth fairly by regulating wait times of traffic classes in proportion according to given weights [15]. Used parameters for both approaches are contention window size, backoff algorithm and inter frame space. The main service differentiation mechanism is the upcoming 802.11e standard. A new access method called Hybrid Coordination Function (HCF) is introduced. It is a queue-based service differentiation that uses both DCF and PCF enhancements. HCF describes some enhanced QoS-specific functions, called contention-based HCF channel access and polling-based HCF access channel. These two functions are used during both contention and contention free periods to ensure QoS. Enhanced DCF (EDCF) is the contention-based HCF channel access. The goal of this scheme is to enhance DCF access mechanism of IEEE 802.11 and to provide a distributed access approach that can support service differentiation. The proposed scheme provides capability for up to eight types of traffic classes. It assigns a short contention window to high priority classes in order to ensure that in most cases, high priority classes will be able to transmit before the low-priority ones. For further differentiation, 802.11e proposes the use of different IFS set according to traffic classes. Instead of DIFS, an Arbitration IFS (AIFS) is used. Classes with smallest AIFS will have the highest priority.

Admission Control and Bandwidth Reservation. Service differentiation is helpful in providing better QoS for multimedia data traffic under low to medium traffic load conditions. However, due to the inefficiency of IEEE 802.11 MAC, service differentiation does not perform well under high traffic load conditions [12]. In this case admission control and bandwidth reservation become necessary to in order to guarantee QoS of existing traffic. These two approaches are quite difficult to realise due to the nature of the wireless link and the access method. Admission control schemes can be broadly classified into measurement-based and calculation-based methods. In measurement-based schemes, admission control decisions are made based on the measurement of existing network status, such as throughput and delay. On the other hand, calculation-based schemes construct certain performance metrics or criteria for evaluating the status of the network [15].

Link Adaptation. 802.11 specify multiple transmission rates but it intentionally leaves the rate adaptation and signalling mechanisms open. Since transmission rates differ with the channel conditions, an appropriate link adaptation mechanism is desirable to maximize the throughput under dynamically changing channel conditions [15]. Most link adaptation mechanisms focus on algorithms to switch among transmission rates specified in the Physical Layer Convergence Procedure.

These different mechanisms aiming to enhance the quality of service support in the IEEE 802.11 wireless LAN treat the network locally. For example parameters differentiations are made at the node level. The keystone of our approach is to consider the wireless LAN as a hole. We try to make a fair distribution of the load among overlapping cells. So we can fulfil an increasing number of accepted applications with guaranteed quality of service level.

3 General Approach Presentation

The QoS management on hotspots environment becomes vital for many new emerging applications such as mobile information access, real time multimedia communications, networked games, immersion worlds and cooperative work. These require a minimum level of QoS [7], [8], [12] and [13]. The hotspots environment can be described as a set of access points covering overlapping cells and offering connection to a variable number of mobile stations. User's applications are not similar in terms of QoS requirements so that a fair distribution of the mobile stations among active access points can guarantee a minimum level of quality of service. The bandwidth effectively offered (C_{max}) by an access point is given by Shannon formula (C_{max} = BP x $\log_2$ (1 + S/N) where BP is the bandwidth and S/N the signal-to-noise ratio). So, due to the wireless environments (interferences, obstacles…) bandwidth is scare and channel conditions will be time-varying and sometimes highly lossy. Unfortunately, in the actual IEEE 802.11 protocol, a mobile station is associated to the access point offering the best Signal-to-Noise Ratio (SNR) independently of the load being applied to the access point by other users. This can cause, in many cases, unbalanced load between access points. Some access points will be over loaded, others are under loaded. For the first ones applications requirements are not fulfilled. The keystone of our approach is to associate mobile station to access points with a minimum SNR threshold and offering the best QoS level.

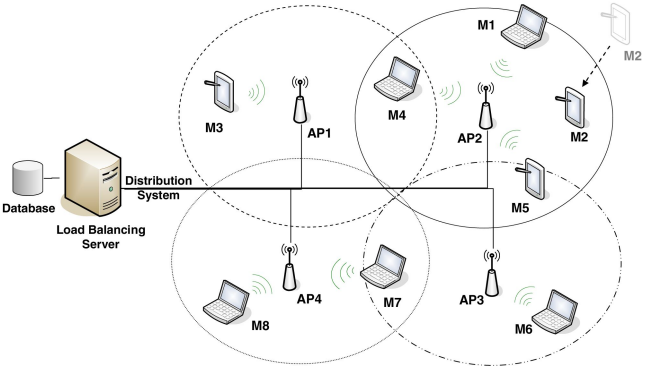


Fig. 1. IEEE 802.11 target architecture

Figure 1 illustrates the idea that we develop in this paper. A new mobile station (M2) reaching the WLAN must be associated with an AP. The association procedure is always initiated by the station (mobile-controlled handover) and the station can be associated with only one AP. The new station must discover which APs are present and then requests to establish an association with one of them. Thus, first the station initiates a scanning process that can be either active or passive [3]. Once the scanning process has finished, the station updates its list of access points in range (AP2).

This information is used by the station to associate with the access point that provides the highest SNR. M2 have to associate with AP2. Supposing that all mobile stations generate the same data traffic, the load distribution across access points will

be highly uneven [1]. This can cause a performance degradation perceived by the other stations attached to AP2. Quality of service contracts (bandwidth, loss rate…) may be violated. It will be attractive to redistribute mobile stations among APs even with lower SNR. A fair distribution of mobile stations among APs fulfills the QoS requirements of both old and recent associated stations: the available bandwidth of the WLAN link depends strongly on the number of active stations and their traffic. To achieve this balancing, in terms of quality of service offered to the stations (load, loss rate…) among APs, we have to compute a balancing algorithm each time a new event such as the arrival of new stations or the mobility of existing stations. This algorithm has to find the best state of associations between APs and mobile stations that offers the best quality of service level for user's applications. Thus, we have to get information on associated stations, traffic coursed by APs and users quality of service requirements (Figure 2). This information has to be exchanged between WLAN entities and stored in an updated data base.

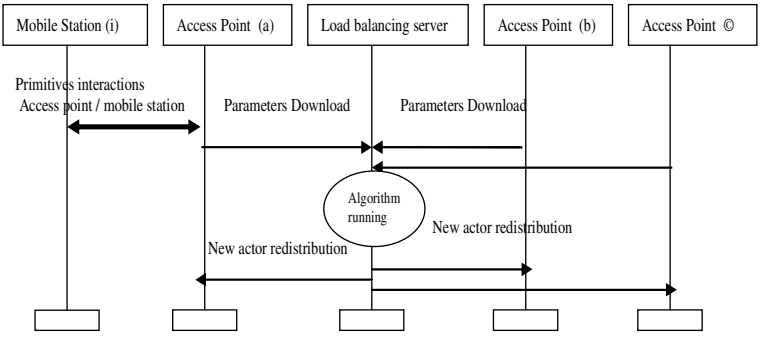


Fig. 2. System protocol interactions

In this architecture the load balancing server should periodically download a set of specific parameters from each access point. It executes the balancing algorithm in order to find the best mobile station distribution among access points. The result will be broadcasted in the system. Then, we have defined for this architecture a set of new metrics to quantify the quality of service and primitives to exchange these parameters for association and disassociation between mobile station and access point. These primitives that should be inserted into the MAC layer to improve the IEEE 802.11 standard [9] define a new MAC quality of service policy for wireless LANs.

4 Load Balancing Algorithm Description

The load balancing algorithm [10], [11] is computed by the load balancing server every time a new distribution is needed in the wireless LAN. This will occurred (i) when a new mobile station enters the wireless LAN and aims to associate with an access point, (ii) when an associated station is moving from one to another BSS and (iii) when the applications requirements in a mobile station are changing. The downloaded parameters from the access points and mobile station applications will be

useful to find the best distribution of mobile stations among wireless LAN access points. This algorithm checks if the new distribution is balanced mainly by computing the balance index (β). The balance index appeared in the first time in [6] and it is used in [2], [10] as a performance measure. The balance index reflects the used capacity in each access point. Let Ti be the total traffic of the APi. Then, the balance index is:

$$\beta j = (\Sigma_i Ti)^2 / (n*\Sigma_i Ti^2)$$

With βj is the balance index of an overlapping zone j, Ti is the total traffic of an APi overlapping with other access points in the zone j and n is the number of access points overlapping in the zone j.

The proposed distribution of mobile stations is balanced if the balance indexes of all the overlapping cells converge to 1. At this step, the algorithm has to send the new distribution to the access points which will be dissociate, associate and reassociate mobile stations.

5 Protocol Specification

5.1 QoS Protocol Parameters

In this approach, the QoS management is based on the idea that some added primitives must be ensured at the connection level between the mobile station and the access point. Then, each mobile in the wireless LAN may be able to propose a level of QoS and to modify it when needed. In this architecture, the mobile station defines four variables managing its QoS state. The communication process will then base its negotiation with the access point on these parameters to build up clause for service quality. Table 1 sums up these parameters and their functions.

Table 1. Quality of service parameters

Parameter	Function
QoS_{max}	The maximum quality of service that the mobile station can offer to the user
$QoS_{negociated}$	The quality of service used by the mobile station at time t
$QoS_{expected}$	The quality of service wanted by the user or the application
$Old\_QoS_{negociated}$	It is necessary to conserve the old quality of service to make comparisons in case of voluntary changes or new offers of QoS.

The following inequality describes the logical relation between these parameters

$$QoS_{max} \geq QoS_{expected} \geq QoS_{negociated}$$

From the part of the access point, some other parameters must be provided to enable QoS management (Table 2).

So, we can propose rules that enable the management of the stations access according to the requirements and the availability of QoS:

$$D_r = D_u + QoS_{expected} \text{ and } D_r < D_{max} - D_{min}$$

Table 2. Access point parameters

Parameter	Function
D_{max}	The higher throughput that can be provided by the access point according to his hardware capabilities
D_{min}	The lower throughput agreed for each user (the Best Effort service)
Da	The reserved throughput, that means the required throughput for a mobile station in an attachment attempt added to the current throughput
D_r	The reserved throughput, that means the required throughput for a mobile station in an attachment attempt added to the current throughput.

5.2 Device Identification

In this approach, to ensure QoS management in the WLAN some identifiers should be joined to the parameters describing present and old quality of service states in each mobile. These identifiers are maintained in a specific database both in the access point and the mobile station. Each mobile station will then discuss the attachment attempt responses of the access point according to its own QoS parameters. We describe in table 3 these parameters from both the access point and the mobile station point of view.

Table 3. New wireless entities parameters

Parameters	Access point	Mobile Station	Function
My_Id_{AP}	*		The access point identifier
$Id_M(X)$	*		The identifier of mobile station number X
My_Id_M		*	Defines the mobile station identifier
$QoS_{negociated}(X)$	*	*	The Quality of service negotiated with the mobile station X
$Old\_QoS_{negociated}(X)$	*	*	The old level of QoS being agreed for a mobile station number X
St_Moving(X)	*		Describes the state of moving state of the X mobile station
St_Reserved(X)	*		Describes presence state of the mobile station X
Timer(X)	*	*	For actions limited in time

These parameters have to be saved in a specific data base managing the whole environment of the wireless device. This database communicates with the other layers defined in the IEEE 802.11 model to ensure coordination in call admission processes.

5.3 QoS Protocol Primitives

The IEEE 802.11 suffers from lack of specific QoS primitives. The only parameter on which is based the connection negotiation between the AP and the mobile station is the SNR ratio. The satisfaction of only this parameter in the connection phase don't meet necessary the QoS requirements of the application. So it appears indispensable to specify new protocol primitives to enable the integration of other communication

parameters in the connection decision and then in loading redistribution. We have then, defined a set of new primitives expressing general requirements.

Table 4. Quality of service primitives

Primitives	Access Point	Mobile Station	Parameters
ASK_ATTACH.conf	*		(Id_M, Id_{AP}, $QoS_{negociated}$)
ATTACH.conf:	*		(Id_M, Id_{AP}, $QoS_{negociated}$)
WAIT	*		(Id_M, Id_{AP})
ASK_RATTACH.req	*		(Id_M, Id_{AP}, available_APs)
ASK_ATTACH.req		*	(Id_M, Id_{AP}, $QoS_{expected}$)
ATTACH.req		*	(Id_M, Id_{AP}, $QoS_{negociated}$)
ATTACH.req		*	(Id_M, Id_{AP}, $QoS_{negociated}$)
ASK_RATTACH.conf		*	(Id_M, New_Id_{AP}, Old_Id_{AP})
LEAVE		*	(Id_M, Id_{AP})
OK	*	*	(Id_M, Id_{APa}, Id_{APb})
MOD_QoS.req	*	*	(Id_M, Id_{AP}, $QoS_{proposed}$, time)
MOVE.req	*	*	(Id_M, Id_{AP})
MOVE.conf	*	*	(Id_M, New_Id_{AP}, Old_Id_{AP})

6 Scenario Description

The primitives that we defined in the last section are used to manage the access of the mobile stations to the wireless LAN via access points. Then we check theses

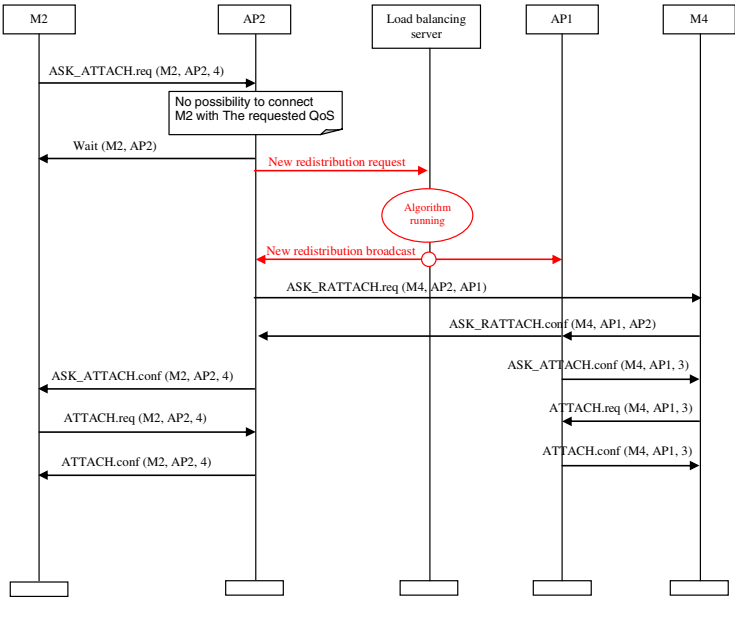


Fig. 3. Example of communication scenario

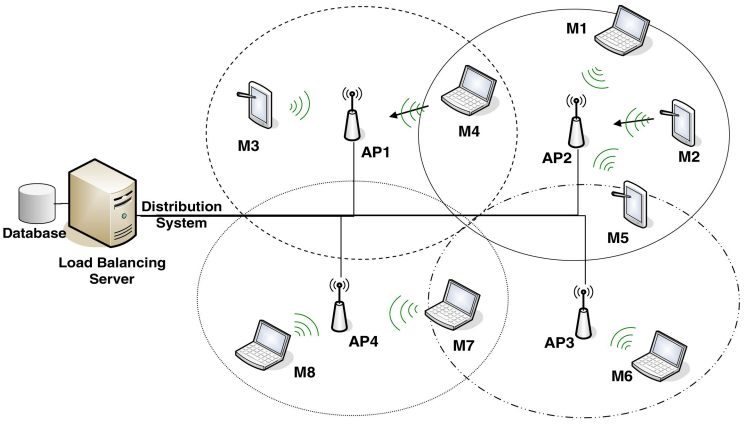


Fig. 4. M2 connected to AP2

primitives with many communications scenarios. Communications scenarios vary from simple to much complex situations. In this paragraph we describe one of the scenarios. We take as example the wireless topology described in Figure 1. Once M2 arriving to the AP2 cell, the load balancing algorithm is computed. The load balancing server broadcasts the new distribution of mobile stations onto the access points. AP2 have to dissociate a mobile station M4. This one will be associated to AP1 which is able to give it the required quality of service level. Finally M2 and AP2 complete the connection procedure (Figure 3) to obtain the balanced wireless network topology (Figure 4).

The scenarios that we have defined will be described and verified with the SDL and MSC languages in the following sections.

6.1 SDL Protocol Description

The SDL pattern is an efficient design language for the development of a communication system. It enables a formal description system by defining a static modular architecture and interactions between different blocks [4]. Systems in SDL language are structured into interconnected entities (system, block, process, and

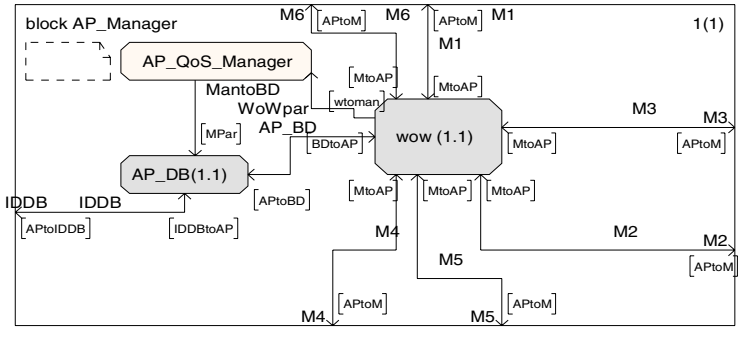


Fig. 5. SDL model of a mobile station

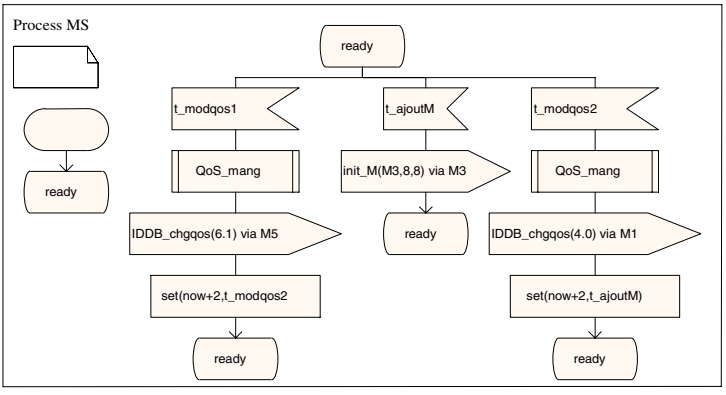


Fig. 6. Example of SDL EFSM development

channel) where process system description provides dynamic behaviour for internal task execution. It is based on the model of Extended Finite State Machines (EFSMs) [5]. In its dynamic behaviour, each state is reached after asynchronous signal exchange between blocks.

New primitives and exchanges defined in our approach have been described and validated with SDL (Figs. 5 and 6). Figure 5 shows the SDL model of a mobile station. It represents exchanges between the management layer and the data base of the mobile station.

6.2 MSC Verification and Simulation

To check the QoS protocol behaviour based on the defined communication scenarios such as the one defined in Figure 3, we have used the ObjectGeode tool based on SDL

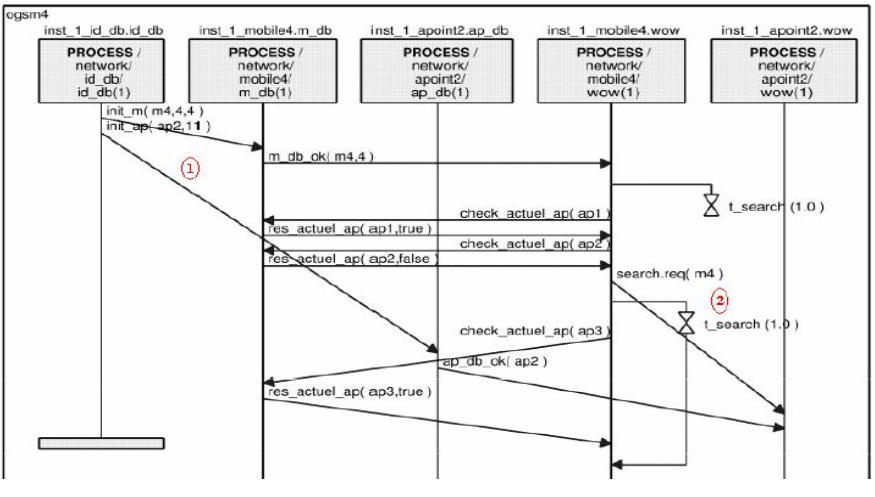


Fig. 7. MSC simulation of an example of exchange between wireless entities

and MSC. With SDL, we have validated the new primitives' exchanges between access points and mobile stations. The Figure 7 brings out a part of simulation results of a QoS negotiation between a mobile station (mobile 4) and an access point (AP2). First of all, entities must be set. Here we have a new instance of the mobile station M4 and the access point AP2. Mobile station gets his identifier, QoS_{max} and $QoS_{expected}$ values and begins a search of the access point with the requested QoS. Some other communication scenarios are also verified with SDL and MSC.

7 Conclusion and Future Works

This paper addresses the problem of QoS management in the WLAN. It presents a protocol specification between mobile stations and access points to negotiate QoS requirements during the mobile station attachment. This protocol defines some new primitives related to the QoS management that must operate with the IEEE 802.11. The specification of these protocol primitives has been carried out. The second part of this paper presents an SDL description of this protocol and it shows the behavior verification with MSC simulation.

This work has to be completed with an implementation of this approach in a simulation architecture using an appropriate tool such as Opnet or Network Simulator (NS). This helps to analyze the performances and helps to adjust the parameters of this protocol before the experimentation. Other parameters can be also used to characterize quality of service requirements of the mobile stations such as loss ratio or jitter.

Acknowledgement

This work has been performed with the finance support of the CMCU project: an integrated action between Tunisian and French Ministry cooperation. This project aims the study of QoS management in distributed systems (Wireless and NoC systems).

References

1. Balachandran, A., Voelker, G.M., Bahl, P., Rangan, P.V.: Characterizing User Behavior and Network Performance in a Public Wireless LAN. ACM SIGMETRICS Int. Conference on Measurement and Modelling of Computer Systems. Marina Del Rey, California (2002)
2. Balachandran, A., Voelker, G.M., Bahl, P.: Hot Spot Congestion Relief in Public-Area Wireless Networks. 4th Workshop on Mobile Computing Systems and Applications. Callicoon, New York, USA (2002) 70-80
3. Matthew, S. G.: 802.11 Wireless Networks : The Definitive Guide. 1st edn. O'Reilly and associates Inc (2002)
4. Gotzhein, R., Schaible, P.: Pattern-based Development of Communication Systems. Annales Télecommunication, N° 54 (1999)

5. Probert, R.L., Ural, H., Williams, A.W.: Rapid Generation of Functional Tests Using MSCs, SDL and TTCN. Computer Communications, Vol. 24 No. 3-4. Elsevier (2001) 374–393
6. Chiu, Dah-Ming, Jain, : Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks. Journal of Computer Networks and ISDN, Vol. 17, N. 1. (1989) 1-14
7. Ni, Q., Romdhani, L., Tureletti, T.: A Survey of QoS Enhancements for IEEE 802.11 Wireless LAN. Journal of Wireless Communications and Mobile Computing, Vol. 4, Issue 5. John Wiley and Sons Ltd (2004) 547-566
8. Lin, C. R., Gerla, M.: Real Time Support in Multihop Wireless Networks. ACM Wireless Networks, Vol. 5, N. 2. ACM (1989) 125-135
9. IEEE 802.11 WG. ANSI/IEEE Std 802.11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications : medium access control (MAC) Enhancements for quality of service (QoS) IEEE 802.11/D2.0. (2001)
10. Velayos, H., Aleo, V., Karlsson, G.: Load Balancing in Overlapping Wireless Cells. International Conference on Communications. IEEE, Paris, France (2004)
11. Bianchi, G., Tinnirello, I.: Improving Load Balancing Mechanisms in Wireless Packet Networks. Int. Conference on Communications. IEEE, New York, USA (2002) 891-895
12. Lindgren, A., Almquist, A., Schelen, O.: Evaluation of Quality of Service Schemes for IEEE 802.11 Wireless LANs. Annual Conference on Local Computer Networks. IEEE, Tampa, Florida, USA (2001) 348-351
13. Mangold, S., Choi, S., May, P., Klein, O., Hiertz, G., Stibor, L.: IEEE 802.11e Wireless LAN for Quality of Service. European Wireless, Vol. 1. Florence, Italy (2002) 32-39
14. IEEE 802.11 - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS), IEEE 802.11e/Draft 4.2. (2003)
15. Zhu, H., Li, M., Chlamtak, I., Prabhakaran, B.: A survey of Quality of Service in IEEE 802.11 Networks. Wireless Communications, Vol. 11, No. 4. IEEE (2004) 6-14
16. Pattara-Atikom, W., Krishnamurthy, P., Banerjee, S.: Distributed Mechanisms for Quality of Service in Wireless LAN. Wireless Communications, Vol. 10. IEEE (2003) 26-34

Stable and Energy Efficient Clustering of Wireless Ad-Hoc Networks with LIDAR Algorithm

Damianos Gavalas[1], Grammati Pantziou[2], Charalampos Konstantopoulos[3], and Basilis Mamalis[2]

[1] Department of Cultural Technology and Communication,
University of the Aegean Greece
dgavalas@aegean.gr
[2] Department of Informatics, Technological Education Institute of Athens, Greece
{pantziou, vmamalis}@teiath.gr
[3] Computer Technology Institute, Patras, Greece
konstant@cti.gr

Abstract. The main objective of clustering in mobile ad-hoc network environments is to identify suitable node representatives, i.e. cluster heads (CHs) to store routing and topology information; CHs should be elected so as to maximize clusters stability, that is to prevent frequent cluster re-structuring. A popular clustering algorithm (LID) suggests CH election based on node IDs (nodes with locally lowest ID value become CHs). Although fast and simple, this method is biased against nodes with low IDs, which are likely to serve as CHs for long periods and are therefore prone to rapid battery exhaustion. Herein, we propose LIDAR, a novel clustering method which represents a major improvement over traditional LID algorithm: node IDs are periodically re-assigned so that nodes with low mobility rate and high energy capacity are assigned low ID values and, therefore, are likely to serve as CHs. Our protocol also greatly reduces control traffic volume of existing algorithms during clustering maintenance phase, while not risking the energy availability of CHs. Simulation results demonstrate the efficiency, scalability and stability of our protocol against alternative approaches.

1 Introduction

Current wireless cellular network infrastructures rely on a wired backbone connecting base stations, implying that networks are fixed and constrained to a geographical area with a pre-defined boundary. Deployment of such networks takes time and cannot be set up in times of utmost emergency. Therefore, mobile multi-hop radio networks, known as mobile ad hoc networks (MANETs), play a critical role in places where a wired (central) backbone is neither available nor economical to build, such as law enforcement operations, battle field communications, disaster recovery situations, and so on [15]. Such situations require a dynamic network topology where all nodes, including routers, are mobile and communication between two end nodes can be supported by intermediate nodes.

Dynamic routing is a key issue in MANETs design and deployment. However, it has been proved that a flat structure exclusively based on proactive or reactive routing

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 100 – 110, 2006.

schemes encounter scalability problems with increased network size, especially in the face of node mobility [10]. One promising approach is to build hierarchies among the nodes, such that the network topology can be abstracted. This process is commonly referred to as *clustering* and the substructures that are collapsed in higher levels are called *clusters* [3]. Clustering not only makes a large MANET appear smaller, but more importantly, it makes a highly dynamic topology to appear less dynamic [12].

In clustering procedure, a representative of each cluster is 'elected' as a *cluster head* (CH) and a node which serves as intermediate for inter-cluster communication is called *gateway*. Remaining members are called *ordinary nodes*. CHs hold routing and topology information, relaxing ordinary mobile hosts (MHs) from such requirement; however, they represent network bottleneck points and -being engaged in packet forwarding activities- are prone to fast battery exhaustion. The boundaries of a cluster are defined by the transmission area of its CH.

A considerable body of literature has addressed research on MANETs clustering; many algorithms that consider different metrics and focus on diverse objectives have been proposed [1][2][6][8]][9][11]. Existing algorithms typically separate clustering into two phases, *cluster formation* and *cluster maintenance*, throughout the latter phase, initial cluster configurations may be modified, depending on nodes movement [10]. However, some clustering schemes employ explicit message exchange among MHs in *periodic* basis for maintaining the cluster structure [8][9][11]; that is, cluster formation is repeated at the end of each period resulting in excessive consumption of network resources. Yet, even the algorithms that apply a different cluster maintenance method may cause the cluster structure to be completely rebuilt over the whole network when some local events take place, e.g. the movement or "die" of a MH, resulting in some CH re-election (re-clustering) [1][2]. This is called the *ripple effect* of re-clustering, which indicates that the re-election of one CH may affect the structure of many clusters and arouse the CH re-election over the network [4]. For clustering schemes with ripple effect, the communication complexity for the re-clustering in the cluster maintenance phase may be the same as that in the cluster formation phase and greatly affect the performance of upper-layer protocols.

In this article, we introduce a protocol for efficient and scalable clustering of MANETs designed with two main objectives in mind:

- Fast and inexpensive completion of clustering formation; our clustering algorithm incorporates both mobility and battery power metrics so that only MHs with low mobility and sufficient energy availability are likely to be elected as CHs; to meet this objective, we have extended a traditional clustering algorithm [11], described in the following section.
- Cost-effectiveness and 'fairness' in cluster maintenance; our algorithm aims at minimizing control traffic and enhance cluster stability, yet, not to prolong CHs serving time and cause rapid exhaustion of their energy supplies.

The remainder of the paper is organized as follows: Section 2 overviews related work and explains the motivation for our research. Section 3 describes the details of our proposed protocol, while Section 4 discusses simulation results. Finally, Section 5 concludes the paper and draws directions for future work.

2 Related Work and Motivation

Several heuristics have been proposed to address ad-hoc networks clustering problem. One of the most popular ones is the Lowest-ID (LID) [11], wherein each node is assigned a unique ID. Periodically, nodes broadcast their ID through a 'Hello' control message, within a period termed the 'Hello period' (HP). The lowest-ID node in a neighborhood is then elected as the CH; nodes which can 'hear' two or more CHs become gateways, while remaining MHs are considered as ordinary nodes.

Highest-Degree (HD) algorithm, originally proposed in [9], uses exclusively location information for cluster formation: the highest *degree* node in a neighborhood, i.e. the node with the largest number of neighbors, is elected as CH. Experiments have demonstrated that HD-based clustering suffers from poor cluster stability: the highest-degree node (the current CH) may fail to be re-elected even if it looses a single neighbor [2].

Vote-based clustering (VC) [8] uses both degree and power level information for CHs election, so as to prevent electing CHs with insufficient energy supply. However, simulation results reported in [8] revealed that the inclusion of the degree metric certainly affects clusters stability, similarly to HD algorithm.

The main asset of LID method is its implementation simplicity. It is also a quick clustering method, as it only takes two HPs to decide upon cluster structure and also provides a more stable cluster formation than HD. In contrast, HD and VC need three HPs to establish a clustered architecture [8]. However, the main drawback of LID heuristic is its bias towards nodes with smaller IDs: these nodes are highly likely to serve as CHs for long periods which may lead to their rapid battery drainage. In addition, neither LID nor HD algorithm take into account mobility metrics, i.e. highly mobile nodes are equally likely to be elected as CHs, although their movement away from their attached cluster members may soon lead to a ripple re-clustering effect [17]. Most importantly, LID, HD and VC do not cater for separating cluster maintenance phase, i.e. CHs election takes place *periodically*; that scheme consumes considerable bandwidth so that upper-layer applications cannot be implemented due to the inadequacy of available resources.

The Weighted Clustering Algorithm (WCA) [2] employs combined-metrics-based clustering: a number of metrics, including node degree, CH serving time (to estimate residual energy capacity) and moving speed, are taken into account to calculate a weight factor I_v for every node v. Mobile nodes with local minimum I_v are elected as CHs. CHs election process is invoked: (a) at the very beginning of cluster formation; (b) during cluster maintenance, when a mobile node moves to a region not covered by any CH. WCA does not invoke re-clustering when a member node changes its attaching cluster. Even though this mechanism can enhance the stability of cluster topology, this also implies that CHs keep their status without considering the attribute of minimum I_v in later cluster maintenance. For instance, in relatively static networking environments, WCA will hardly ever be invoked, hence CHs service time will be prolonged and elected CHs will soon suffer from battery exhaustion. Also, article [2] does not clarify how MHs re-affiliation takes place, i.e. the process for the detachment of a MH from its current CH and the attachment to another [17].

3 Description of Our Proposed Protocol

In this article, we propose a novel clustering protocol, Lowest-ID with Adaptive ID Reassignment (LIDAR). LIDAR explicitly separates cluster formation and cluster maintenance phases through employing two distinct algorithms. The former extends LID algorithm's approach to identify the most suitable CHs among MANET nodes in a fast and inexpensive manner. The latter aims at minimizing cluster re-formation occurrences, yet not at the expense of frequent network disconnections owned to CHs energy depletion. These two algorithms are presented in the following two sections.

3.1 Cluster Formation Algorithm

The main idea behind LIDAR's cluster formation method is to maintain the assets of LID algorithm (fast, simple and low-cost clustering process) while providing stable clusters and catering for balanced computational load and power consumption among mobile nodes. This is achieved through identifying and electing the most suitable nodes as CHs, i.e. those with sufficient power level and low mobility rate.

MHs in a MANET normally depend on battery power supply, therefore energy consumption should be reduced in order to prolong the network lifespan [18]. Also, a CH bears extra work compared with ordinary members, and it is likely to "die" early because of excessive energy consumption. The lack of MHs due to energy depletion may cause network partition and communication interruption [3]. Hence, it is also important to balance the energy consumption among nodes to avoid node failures, especially when the network density is comparatively sparse.

In addition, mobility is a prominent characteristic of MANETs, and is the main factor affecting topology change and route invalidation [12][16]. MHs that exhibit high mobility are inadequate for serving as CHs since their movement is likely to trigger frequent re-clustering, therefore increasing control traffic volume.

Therefore, our cluster formation algorithm takes into consideration both energy availability and mobility metrics to prolong network lifetime and avoid unnecessary re-clustering (i.e. enhance clusters stability). We have chosen not to include a node degree metric, as this has been shown to negatively affect cluster stability [6][8][17]. LIDAR's execution involves the following steps:

Step 1: At startup, node IDs are arbitrarily assigned. Initial clustering of mobile nodes is performed using LID algorithm, chosen due to its simplicity, fast and inexpensive completion of clustering process.

Step 2: At the end of every HP, each mobile node v calculates the following weighted function value:

$$W_v = w_1 B_v - w_2 M_{v,t}, \quad w_1 + w_2 = 1 \tag{1}$$

where B_v denotes the remaining battery life of node v and $M_{v,t}$ represents the mean mobility rate of node v during the latest p HPs, where p is a small integer (in the following sub-section, we describe how mobility rate is measured).

Step 3: Whenever re-clustering is needed (in the following section we discuss the circumstances under which re-clustering process is triggered), CHs request their

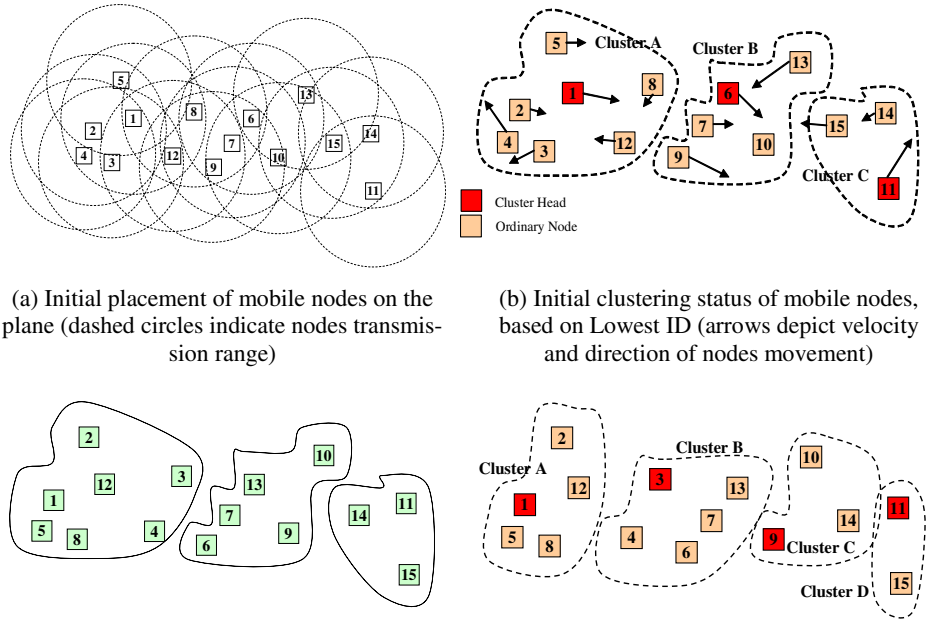
attached MHs to send their W_v values through a special broadcast message (WEIGHT_REQUEST).

Step 4: W_v values are unicasted by MHs to their local CH through a WEIGHT_REPLY message along with B_v values (the later are used during cluster maintenance phase).

Step 5: Having received W_v values from their attached cluster members, CHs sort them in descending order and re-assign node IDs so that small IDs are assigned to nodes with larger W_v values and large IDs to nodes with smaller W_v values. Namely, lower IDs are assigned to nodes with high power level and low mobility rate, thereby increasing their probability of being elected as CHs in the next algorithm's step.

Step 6: CHs send to their attached members their respective new_ID values.

Step 7: Mobile nodes update their ID values. Right after, re-clustering procedure is invoked, where clusters formation is based on LID algorithm (go back to Step 1).



(a) Initial placement of mobile nodes on the plane (dashed circles indicate nodes transmission range)

(b) Initial clustering status of mobile nodes, based on Lowest ID (arrows depict velocity and direction of nodes movement)

(c) Re-assignment of node IDs within individual clusters

(d) Re-clustering of mobile nodes, based on Lowest ID

Fig. 1. Illustration of LIDAR execution steps

Upon completion of cluster formation, the protocol 'switches' to the cluster maintenance phase, i.e. control traffic is no longer exchanged until cluster formation process is re-invoked (details are given in the following section). LIDAR execution steps are illustrated in Fig. 1. Table 1. presents how W_v values are calculated, where the coefficients of equation (1) are set to $w_1 = 0.7$ and $w_2 = 0.3$:

Table 1. Calculation of W_V values and node IDS re-assignment in LIDAR (where $w_1 = 0.7$ and $w_2 = 0.3$)

	Node ID	B_v	$M_{v,P}$	W_v	New Node ID
Cluster A	1	2	4	0,2	12
	2	7	1	4,6	1
	3	4	3	1,9	8
	4	6	4	3	5
	5	7	2	4,3	2
	8	6	1	3,9	3
	12	6	2	3,6	4
Cluster B	6	3	3	1,2	13
	7	7	2	4,3	7
	9	8	4	4,4	6
	10	6	0	4,2	9
	13	7	4	3,7	10
Cluster C	11	3	4	0,9	15
	14	6	1	3,9	11
	15	6	2	3,6	14

Most existing methods for estimating nodes mobility rate pose the requirement for GPS card with sufficient accuracy mounted on every mobile node. We propose an alternative method for measuring mobility rate which relaxes mobile nodes from such requirement. In particular, each CH measures its neighborhood mobility rate through contrasting the topology information it obtains during successive HPs.

A main objective of LIDAR algorithm is to minimize control traffic overhead during clustering formation phase, which highly depends on HP duration (i.e. frequency of broadcasting 'Hello' control packets). To achieve that, CHs measure the mean mobility rate of their attached cluster members MRc and accordingly adapt the 'Hello' broadcast period BP within their cluster. It is also guaranteed that HP duration always lies between two boundaries: $HP_{\min} \leq HP \leq HP_{\max}$; at startup, HP is globally set to $HP_{\min}$. The details of our mobility rate measurement method may be found in [7].

3.2 Cluster Maintenance Algorithm

The main criticism against cluster-based structures in MANETs focuses on the need for extra explicit message exchange among MHs for maintaining the cluster structure [10]. When network topology is highly dynamic, resulting in frequent cluster topology updates, the control overhead of cluster maintenance increases drastically. Thus, clustering operation may consume a large portion of network bandwidth, drain mobile nodes' energy quickly, and override its improvement on network scalability and performance [13]. By limiting re-clustering situations or minimizing explicit control messages for clustering, the cluster structure can be maintained well without excessive consumption of network resources [17].

Our cluster maintenance algorithm, follows an approach whereby clustering is not executed periodically but in an *event-driven* manner. That is, re-clustering process is only invoked when an important event occurs:

(a) The Energy Level of a CH has Significantly Decreased
Each elected CH holds information about its node degree d and also the battery level B_v of its cluster members at the election time (see step 4 of cluster formation algorithm). Nodes serving as CHs for a long period of time are expected to drop their battery level B_{CH} faster than ordinary nodes. To prevent the risk of energy depletion, CHs periodically check their B_{CH} value. When B_{CH} falls far below the average energy level of CH's cluster members, i.e. when $B_{CH} < T * \frac{\sum_{v=1}^{d} B_v}{d}$ (where T ≤ 1), the CH invokes a cluster formation process; namely, the CH is soon replaced by another node with higher energy availability. Unlike the method proposed in [2], our approach ensures that CH role is fairly shared among MHs regardless of the MANET's topology characteristics, hence energy consumption is uniformly distributed. It should also be stressed that our proposed scheme does not cause a ripple of re-clustering effect, since only CHs with decreased battery level relinquish their CH role, without affecting neighboring clusters.

(b) The MANET Topology has Significantly Changed
The highly dynamic nature of MANET topologies combined with infrequent re-clustering implies that cluster structures may soon be outdated. On the other hand, the maintenance of updated cluster formations presupposes frequent exchange of control traffic, which should certainly be avoided. Hence, we propose a scheme whereby cluster formation is invoked when the MANET topology has changed to such extent that CHs are unable to route incoming traffic to its destination node. Following that approach, we ensure that in relatively static MANET topologies (e.g. in convention centers, conferences or electronic classrooms), where relocations of MHs seldom occur, the cost of cluster maintenance is practically eliminated. However, this enormous cost improvement is achieved at the expense of larger setup latency whenever data traffic exchange commences. An alternative method would be to invoke re-clustering whenever a MH re-affiliates (moves away from its attached CH and joins another cluster). Such a method though, would generate excessive control traffic exchange in highly mobile networks for cluster maintenance; in most cases, control traffic would be broadcasted for no reason, e.g. MHs continuously changing their location on the plane, yet, not transmitting any data.

To illustrate our method, let us examine the example topology of Fig. 1.d, which depicts the result of executing our cluster formation algorithm. At a later stage we assume that node #12 issues a data transmission request. At that time, network topology is expected to have changed due to nodes mobility. If this is not the case (topology has remained unchanged), node #1 (nominated as CH of node #12 at cluster formation time) will receive the transmission request and reply sending back an ACK message. Node #12 will than commence data transmission and CH #1 will route received data towards its destination node. If the transmission request is not received by node #1 (either node #1 or #12 has moved away), node #12 will not receive back the

ACK message; as soon as a specified period of time elapses, node #12 will have detected the topology change and trigger a local re-clustering process. The outcome of re-clustering will be the attachment of node #12 to another CH; data transmission will start thereafter. Re-clustering process is 'propagated' along data routing path, if needed. That implies that our approach prevents the ripple re-clustering effect, since re-clustering is only invoked where necessary, i.e. in MANET areas that appear to have significantly reformed.

4 Simulation Results

LIDAR protocol has been simulated using NS-2 simulator [14] and compared against LID, HD and WCA algorithms. Our simulation tests attempt to compare the performance of these algorithms in terms of signaling traffic, cluster stability and variance of MHs energy level.

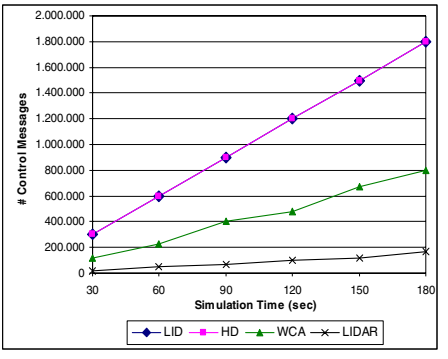
A square terrain of 600m × 600m is assumed. The number of MHs moving within the square space varies from 20 to 120. At startup, MHs are randomly positioned on the plane. MHs move with speed 0 - 15m/s, on random direction. At the event of reaching the terrain boundary, MHs are bounced back. The 'hello period' duration is set to 1 sec for LID, HD and cluster formation phase of WCA and LIDAR approaches. Initial remaining battery time of MHs is randomly set between 20 and 100 units; energy is assumed to be linearly decreased for ordinary nodes, while for CHs it depends on the number of their attached cluster members. Each simulation run lasts 3 minutes; simulation results presented below have been averaged over 5 runs. Regarding the execution parameters of LIDAR, W_v values are calculated for $w_1 = 0.7$ and $w_2 = 0.3$; MHs measure their mobility rate through contrasting the topology information they obtain during $p = 5$ successive 'hello periods' CHs check their battery availability B_{CH} with a period 100 times longer than the 'hello period'.

Fig. 3a illustrates the average number of control messages exchanged as simulation time advances. In LID and HD algorithms, 'Hello' messages are periodically broadcasted during cluster maintenance phase; hence, their performance results coincide. WCA executes re-clustering whenever a MH moves to a region not covered by any CH [2]. On the other hand, the most likely scenario for LIDAR re-clustering is when a MH issues a transmission request. Thus, for reasonable values of average MHs speed (5 m/sec) and average rate of transmission requests (1 request per min for each MH), LIDAR clearly outperforms WCA.

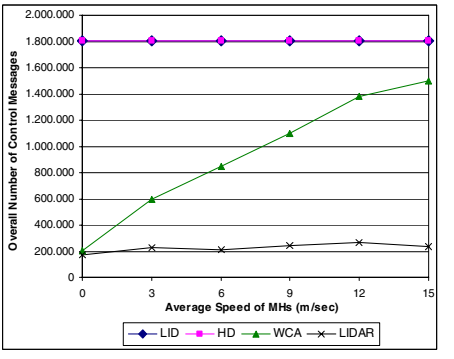
Fig. 3b reveals the dependency of WCA algorithm's performance on the average speed of MHs. Namely, in highly mobile MANET environments WCA involves frequent re-clustering, hence increasing clustering overhead. In contrast, LIDAR's performance remains unaffected; yet, it depends on the frequency of transmission requests.

Fig. 3c compares the average number of CH changes, which is an indicator of the overall cluster structure stability (the more frequent the CH changes, the less stable clusters are). As expected, LID performs better than HD as the former exclusively uses ID and the latter node degree information to decide upon cluster structure. WCA also incorporates degree metric in cluster formation thereby negatively affecting cluster stability; also, as network size increases, it is more likely to invoke re-clustering

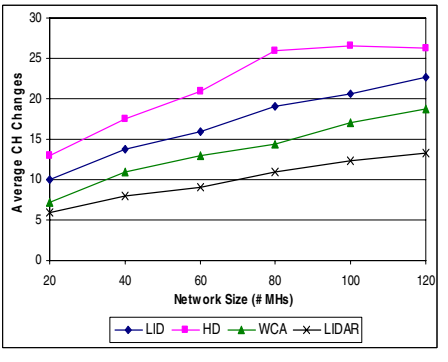
process due to nodes movement. LIDAR provides better results, as it suggests that CH changes do not depend on nodes mobility but may only occur upon data transmission or when CHs run the risk of battery drainage.



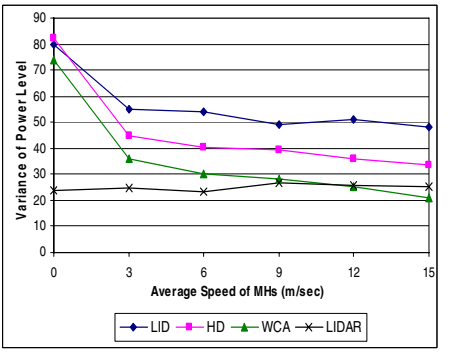
(a) Average number of control messages during simulation runs (50 MHs, with average speed of MHs 5 m/sec and average rate of transmission requests for MHs 1 request/min).



(b) Overall number of control messages (50 MHs, with average rate of transmission requests for MHs 1 request/min).



(c) Average number of CH changes (for average speed of 5 m/sec and average rate of transmission requests for MHs 1 request/min).



(d) Variance of energy level among MHs (50 MHs, with average rate of transmission requests for MHs 1 request/min).

Fig. 2. Simulation results

Finally, Fig. 3d illustrates the variance of power level among MANET's MHs. Large variance values indicate that specific nodes are engaged on CH role for long periods, hence, their energy level soon falls far below the average. This simulation test highlights the main limitation of LID algorithm: in LID, CHs election is biased in favor of nodes with low ID values; these nodes are likely to serve as CHs for long time and their energy supply rapidly depletes. Interestingly though, for static environments (average speed 0 m/sec), LID, HD and WCA algorithms present almost identical variance values among MHs energy level. For LID and HD methods cluster formation is periodically executed only to re-elect the same nodes as CHs (since network topology does not reform). For WCA, following the initial cluster formation, the

lack of nodes movement prevents future re-clustering, hence CHs service time is prolonged and difference between the energy levels of CHs and ordinary nodes increases. However, higher mobility rates imply more frequent triggering of WCA re-clustering events, thereby decreasing variance values. LIDAR exhibits smaller variance of mobile nodes energy level: CHs give up their role even in static environments, when their battery resources are about to exhaust. Namely, CHs role is fairly shared among network nodes, achieving more uniform distribution of energy consumption.

5 Conclusions – Future Work

In this article, we have introduced a novel protocol that explicitly separates clustering process in cluster formation and cluster maintenance phases. The former extends the ideas of LID algorithm increasing the likelihood for electing CHs with low mobility and sufficient energy capacity. The latter aims at minimizing control overhead and enhancing cluster stability, without sacrificing the balanced consumption of energy supplies among MANET nodes.

Simulation results demonstrated that LIDAR protocol outperforms traditional LID and HD algorithms, as well as a more recent approach (WCA) in terms of control traffic overhead, cluster stability and variance of energy level among MHs.

As a future extension, we intend to incorporate mobility metric in the calculation of weight function values, and also introduce a mobility prediction method (e.g. similar to [16]) to identify group mobility patterns and provide steadier cluster formations. The effect of MHs transmission range in the operation of LIDAR will be evaluated for all typical ranges of the standard 802.11a equipment [5]. We also intend to extend our cluster maintenance algorithm so as to restrict the number of nodes dominated by a single CH between a lower and an upper bound; that way, clusters will be small enough to impede drainage of CHs resources and large enough to prevent long routing paths and message delivery delays.

Acknowledgments

The research work presented herein has been co-funded by 75% from EU and 25% from the Greek government under the framework of the Education and Initial Vocational Training II, Programme Archimedes.

References

[1] S. Basagni, “Distributed and Mobility-Adaptive Clustering for Multimedia Support in Multi-Hop Wireless Networks,” Proceedings of the 50th IEEE Vehicular Technology Conference (VTS’99), pp. 889–93, September 1999.

[2] M. Chatterjee, S. K. Das, D. Turgut, “WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks”, Cluster Computing, 5, pp. 193–204, 2002.

[3] Y. P. Chen, A. L. Liestman, J. Liu, “Clustering Algorithms for Ad Hoc Wireless Networks”, in “Ad Hoc and Sensor Networks” (ed. Y. Pan and Y. Xiao), Nova Science Publishers, 2004.

[4] C.-C. Chiang et al., "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel" Proceedings of IEEE SICON'97, pp. 197-211, 1997.
[5] "Cisco Aironet 1230AG Series 802.11a/b/g Access Point Data Sheet", Cisco Systems 2004.
[6] D. Gavalas, G. Pantziou, C. Konstantopoulos, B. Mamalis, "An Efficient and Scalable Clustering Algorithm of Wireless Ad Hoc Networks", Proceedings of the 1st International Workshop on Distributed Algorithms and Applications for Wireless and Mobile Systems (DAAWMS'2005), pp. 761-766, November 2005.
[7] D. Gavalas, G. Pantziou, C. Konstantopoulos, B. Mamalis, "Lowest-ID with Adaptive ID Reassignment: A Novel Mobile Ad-Hoc Network Clustering Algorithm", Proceedings of the 1st IEEE International Symposium on Wireless Pervasive Computing (ISWPC'2006), January 2006.
[8] F. Li, S. Zhang, X. Wang, X. Xue, H. Shen, "Vote-Based Clustering Algorithm in Mobile Ad Hoc Networks", Proceedings of International Conference on Networking Technologies for Broadband and Mobile Networks (ICOIN'2004), LNCS vol. 3090, pp. 13 – 23, February 2004.
[9] M. Gerla, J.T.C. Tsai, "Multicluster, mobile, multimedia radio network", Wireless Networks 1(3), pp. 255–265, 1995.
[10] X. Hong, K. Xu, M. Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks", IEEE Network, 16(4), pp. 11-21, July-Aug, 2002.
[11] C. R. Li, M. Gerla, "Adaptive Clustering for Mobile Wireless Networks", IEEE Journal of Selected Areas in Communications, 15(7), pp. 1265-1275, September 1997.
[12] B. McDonald, F.Znati, "A Mobility-Based Framework for Adaptive Clustering in Wireless Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, Vol. 17, pp. 1466 –1487, August 1999.
[13] B. McDonald, F. Znati, "Design and Performance of a Distributed Dynamic Clustering Algorithm for Ad-Hoc Networks," Proceedings of the 34th Annual Simulation Symposium, pp. 27–35, April 2001.
[14] Network Simulator - NS-2, http://www.isi.edu/nsnam/ns/.
[15] C. Perkins, "Ad Hoc Networking", Addison-Wesley, January 2001.
[16] S. Sivavakeesar, G. Pavlou, A. Liotta, "Stable Clustering Through Mobility Prediction for Large-Scale Multihop Ad Hoc Networks", Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'2004), IEEE, March 2004.
[17] J. Yu, P. Chong, "A Survey of Clustering Schemes for Mobile Ad Hoc Networks", IEEE Communications Surveys, 7(1), pp. 32-48, March 2005.
[18] R. Zheng, R. Kravets, "On-demand Power Management for Ad Hoc Networks," Proceedings.of the IEEE Infocom'2003, pp. 481–91, Mar.–Apr. 2003.

DNS-Based Service Discovery in Ad Hoc Networks: Evaluation and Improvements*

Celeste Campo and Carlos García-Rubio

Dept. de Ingeniería Telemática - Universidad Carlos III de Madrid
Escuela Politécnica Superior - 28011 Leganés (Madrid)
{celeste, cgr}@it.uc3m.es

Abstract. In wireless networks, devices must be able to dynamically discover and share services in the environment. The problem of service discovery has attracted great research interest in the last years, particularly for ad hoc networks. Recently, the IETF has proposed the use of the DNS protocol for service discovery. For ad hoc networks, the IETF works in two proposals of distributed DNS, Multicast DNS and LLMNR, that can both be used for service discovery. In this paper we describe and compare through simulation the performance of service discovery based in these two proposals of distributed DNS. We also propose four simple improvements that reduce the traffic generated, and so the power consumption, especially of the most limited, battery powered, devices. We present simulation results that show the impact of our improvements in a typical scenario.

1 Introduction

The increment in the number of devices connected to networks has motivated the development of service discovery protocols, which help the user in the task of automatically discovering and using the wide range of services available in a network (e.g. printers, mail servers, etc.). Some service discovery protocols have been defined in the IETF for the Internet (SLP [1], SSDP [2]), and others have been defined by other standardization bodies, tied to a particular high-level technology (Jini [3], Salutation [4]). More recently, other service discovery protocols, specifically designed for ad hoc networks, have been defined, some tied to a wireless technology (SDP for Bluetooth [5], IAS for IrDA [6]), others that jointly deal with the problems of ad hoc routing and service discovery (GSD [7], HSID [8]), and others that work at the application layer of the protocol stack (DEAPspace [9], Konark [10], the post-query strategies [11], and PDP [12]). For a complete review of service discovery protocols, see [13].

In their answer messages, service discovery protocols return the name of the server or servers that offer the service, together with other relevant data (e.g. transport protocol, port, service attributes, etc.). Server names are preferred

* This work has been supported by the Everyware (MCyT TIC2003-08995-C02-01) and Easy Wireless (ITEA ip03008) projects.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 111–122, 2006.

to IP addresses because, when there are several responses, the user is usually prompted to select one among them. The device must send a DNS query to resolve the name of the selected server into an IP address, prior to accessing the service.

Recently, the Zeroconf IETF working group has proposed the use of DNS for service discovery, so devices don't need to implement two different protocols (the DNS protocol and a service discovery protocol) but just one for both functionalities. This proposal is known as DNS-Service Discovery (DNS-SD). For ad hoc networks, where service discovery is essential, but the infrastructure necessary to support it may not be always available, DNS-SD can work over any of the two current proposals of distributed DNS for infrastructureless networks: LLMNR and Multicast DNS. In this paper we compare both proposals, evaluating their performance and particularly the traffic they generate.

In wireless networks, one of the key issues is minimizing energy consumption, since most devices are battery powered and so their autonomy is increased. Several studies about power consumption in wireless devices show that wireless communications are responsible of a significant part of the energy consumption, and that the cost of transmitting a packet is almost independent of its size and of whether it is unicast or broadcast [14,15]. These facts must be taken into account when designing protocols for these kind of environments. In this paper, we present some simple improvements that can reduce the traffic generated in DNS based service discovery, and so the power consumed.

The paper is organized as follows. First, section 2 describes the proposals for DNS-based service discovery in ad hoc networks, Multicast DNS and LLMNR. Then, section 3 compares the performance of both proposals through a simulation study, and section 4 proposes some improvements that reduce the number of transmissions and so the power consumption. Finally, section 5 discusses some implementation issues, and, section 6 the conclusions and future work.

2 DNS-Based Service Discovery in Ad Hoc Networks

DNS Service Discovery (DNS-SD) [16] provides support for service discovery over DNS, without making any change to the DNS protocol. With DNS-SD, devices can obtain a list of servers offering a given service type as a response to a DNS query. At the time of writing this paper, this proposal is in Internet Draft state.

DNS-SD works over DNS, so it may use the classical centralized architecture, based on a hierarchy of servers, or any of the DNS modifications for name resolution in infrastructureless networks, Multicast DNS or LLMNR, with a fully distributed architecture.

DNS-SD exploits the syntax and the semantic of the SRV resource records for service discovery, adding one level of indirection to allow the user obtaining instances of service types with different characteristics.

DNS is a protocol that requires network infrastructure and a heavy administrative management due to how domain names are assigned and delegated.

Regardless of whether DNS is being used for service discovery or not, a solution for name resolution in infraestructureless, ad hoc, networks is necessary. Recently, two proposals have been presented in the IETF for distributed DNS, and, as we previously mentioned, they may be also used for DNS-based service discovery: Multicast DNS and Linklocal Multicast Name Resolution.

Both proposals start from the DNS protocol but do out with the centralized architecture, replacing it by a fully distributed approach in which all the devices in the network have their own DNS server, and all DNS queries are multicast. In the following subsections we will describe in detail both proposals.

2.1 Multicast DNS

Multicast DNS [17], as DNS-SD, is fruit of a joint initiative of the Zeroconf and DNSEXT groups of the IETF, with Apple Computer as the prime mover. Multicast DNS defines a new top-level domain, `.local.`. All the names under this domain have meaning only in the local network in which they have been defined. There is no naming authority in charge of managing this domain, but any user or software may create their own names with the `.local.` suffix, provided that they don't clash with names chosen by other users in the same local network.

When the resolution of a name with `.local.` suffix is requested, the Multicast DNS protocol must be used. All devices in the network must have a "Multicast DNS client" that issues multicast resolution queries, and a "Multicast DNS server" that resolves these queries.

In Multicast DNS, applications that request a name resolution can have three modes of operation: "one-shot queries", the client waits for the first response and discards the others; "one query-multiple responses", the client waits for all the answer messages; and "continuous query", in which the client issues the same query periodically, and so it monitors the existence of some resource in the network.

In order to reduce network traffic in the last two modes, queries include all the records previously known by the client (stored in its cache), so a server will answer a query only if it knows of a resource record not included in the query. To include the known records in the query, the answer section of the DNS message is used (the use of the answer section of the message in a query is illegal in classical DNS). If all the known records do not fit in a query packet, this must be signalled setting the TrunCation (TC) bit in the header of the query message, and the rest of the known records must be sent in a new query with an empty query section.

In this protocol, servers send multicast answer messages, so all devices in the network receive all of them, and this way they keep their caches updated. Moreover, this allows fast detection of clashes between domain names used by different devices. To help reducing the number of collisions in the network, servers delay their answer messages to a query a random time uniformly generated between 20–120 ms. All replies must be authoritative answers, so a server never replies with information from its cache.

In Multicast DNS, the TTL (the Time-To-Live defined in DNS) of the resource records is chosen according to how mobile the device is, and how long it will remain in the same network. So, for static devices, large TTL values are configured, and for dynamic devices, small TTL values are used. The recommended default value for the TTL is 120 seconds, which means that other devices in the network may store outdated information about us for up to two minutes. Reducing the TTL reduces the time outdated data remains in the caches when someone leaves the network, but it increases the network traffic.

To reduce the number of stale entries in the cache, and so the number of false service discoveries, Multicast DNS introduces three mechanisms:

- The "goodbye" message: it is used when a server detects that it is about to leave the network or to shutdown. This message consists in a gratuitous answer message (i.e., an answer that do not correspond to any query) in which the device includes all its local resource records (services) with TTL value of zero sec. This way, all devices listening the goodbye message, will delete these records from their caches.
- Update entries: if there is a change in any resource record (e.g., a device changes the characteristics of a service it was offering), the server sends a gratuitous answer message with the updated resource records.
- Remove entries in the local cache: when a failure is detected using the information from a resource record in the cache (e.g., the service does not respond), or a change in the topology of the network is detected, the involved resource resords are removed from the cache.

2.2 Linklocal Multicast Name Resolution

Linklocal Multicast Name Resolution (LLMNR) [18] is an initiative from the DNSEXT group of the IETF, with Microsoft as the prime mover. Its way of approaching the problem of name resolution in ad hoc networks is much more conservative than Multicast DNS, with no modification in the use DNS message fields, and without defining any new domain name for the local scope.

In LLMNR, devices have a "LLMNR client", which sends name resolution queries, and a "LLMNR server", which answers the queries made by the clients.

LLMNR clients transmit their queries using multicast, and wait for answer messages to arrive. Servers which have one or more authoritative resource records that match the query, reply using unicast. Information from the caches cannot be included in the replies. LLMNR is more restrictive than DNS regarding the definition of authoritative zones. In DNS, the authoritative zone of a server comprises all the domain names in the sub-tree under its start of authority (SoA) resource record, except for those delegated to other DNS servers, while in LLMNR a server is authoritative just for the root of its zone and not for the sub-domains under it.

LLMNR uses the same TTL value for all the resource records in a server. This TTL value is chosen depending on how static or dynamic the network is. Larger TTL values reduce network traffic but generate stale cache entries in

highly changing networks. For such networks, such as ad hoc networks, a TTL value of zero is recommended in the draft.

Regarding security aspects, both LLMR clients and LLMNR servers check the source addresses of the reply and query messages received, respectively, before accepting or discarding them. A client only accepts replies from servers with "on-link" IP addresses, i.e., with a source IP address that belongs to the same IP subnetwork as the client. Similarly, a server only answers unicast queries from "on-link" IP addresses, or from multicast queries that use local-scope multicast addresses. Moreover, servers must include in their answer messages just resource records that are reachable from the same subnetwork.

3 Comparative Study of Multicast DNS and LLMNR

Both Multicast DNS and LLMNR keep the DNS message format, syntax and resource record format, although Multicast DNS introduces some changes in the way some of the fields of the DNS message are used (specifically, the use of the answer section in the queries). Regarding the use of these protocols together with DNS-SD to support service discovery, the main differences between both proposals are the following:

- Multicast answers: in LLMNR, servers answer using unicast, while in Multicast DNS they answer using multicast.
- Resource records caches: LLMNR recommends using TTL values of zero for ad hoc environments; therefore, no resource records are cached. Multicast DNS recommends using a TTL value of 120 seconds, and caches are used to improve the operation of the protocol.
- "Goodbye" message: The goodbye message is defined in Multicast DNS. LLMNR does not define an equivalent message. Since a TTL value of zero is recommended in LLMNR for ad hoc networks, no resource records will be stored in caches, and so no false or stale entries are possible.

In this section we will study through simulation the impact that these differences between Multicast DNS and LLMNR have when they are used for service discovery in ad hoc networks. We use OMNeT++[1].

We have simulated an area of 300×300 meters, with a number of devices (clients and servers offering services), all of them mobile, using a Random Way-Point model for the movements, with exponential "thinking times", and an IEEE 802.11 network interface in ad-hoc mode. We have used MAC broadcasts for multicast IP transmissions. Multicast multi-hop ad-hoc routing is not necessary, since both Multicast DNS and LLMNR are defined to be used just on the local link. The length of the simulation was elected to obtain results with a 90% confidence level and a 10% confidence interval.

The variables of our interest are: the number of messages transmitted (normalized per service search), the service discovery ratio (the ratio of services

[1] http://www.omnetpp.org/

discovered), and the service error ratio (ratio of stale or false services discovered).

An optimum service discovery solution for ad hoc networks should achieve as low number of messages transmitted as possible, so reducing power consumption, while keeping a high (close to 100%) service discovery ratio, and a low (close to 0%) service error ratio.

3.1 Multicast Answer Messages and the Use of Caches

In LLMNR, clients send queries using multicast, and servers send their answer messages using unicast; besides, clients are recommended not to make cache of the received answers. In service discovery terminology [12], this mode of operation is commonly known as "pull mode without cache". One of the main advantages of this mode is its reliability and its simplicity. In fact, its performance can be studied analytically. It can be shown that, since each time a service is needed, a query is sent, assuming no link failures, the service discovery ratio is 100%, and the service error ratio is 0%, since all available services respondi the query sent at the time when a service is needed. Given that there are n devices in the network, that each one offers a service, and that there are k different kind of services in the network, the number of messages transmitted per search follows Equation 1.

$$\text{NumberOfMessages} = \frac{k+n-1}{k} \tag{1}$$

Multicast DNS is more complex than LLMNR. Following again service discovery terminology, it behaves as a "pull mode with cache and with multicast responses", or what is equivalent, as a push mode with service announcement's rate controlled by the service request frequency in the network. Moreover, in Multicast DNS, service queries include previously known entries from the cache, what helps to reduce the number of replies necessary for that query.

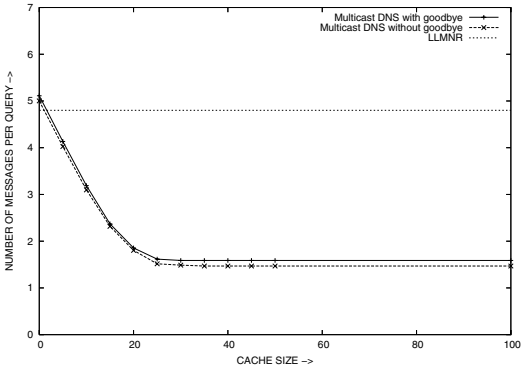
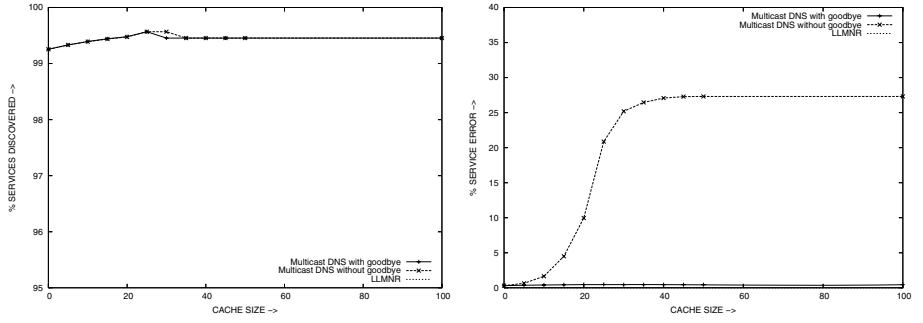


Fig. 1. Number of messages against cache size

Because of its complexity, we have carried out the performance evaluation of Multcast DNS through simulation. The results of these simulations are shown in



(a) (b)

Fig. 2. Service discovery and error percentages against cache size

Figures 1, and 2. The scenario simulated consists of 20 devices in average, each one with an average thinking time of 600 seconds, offering one service, with 5 different kinds of services in the network, and issuing a query (a service request) every 60 seconds in average. We simulate different cache sizes, from 0 to 100 entries (a cache with size n has space to store up to n resource records).

As we can see in Figure 1, this mode of operation significantly reduces the number of messages per service search, compared with LLMNR. The price to pay is that this reduction comes with an increment in the uncertainty about the availability of the services discovered, since although the service discovery ratio reaches the 100%, Figure 2 (a), the service error ratio reaches a value close to 30% when moderate or large caches are used, Figure 2 (b) (plot labelled "Multicast DNS without goodbye")).

3.2 Goodbye Messages

The above mentioned lost of reliability in the Multicast DNS protocol is alleviated through the use of the cache consistency mechanism defined in Multicast DNS. This mechanism allows deleting staled cache entries by using "goodbye" messages. We have repeated the simulations introducing now the use of the "goodbye" message, Figure 2 (plot labelled "Multicast DNS with goodbye"). We see that the service error ratio is reduced to 0% while the increase in the number of messages transmitted is not significant, and continues well under LLMNR, see Figure 1 (plot labelled "Multicast DNS with goodbye").

Considering the results we have obtained, we can conclude that Multicast DNS is more suitable than LLMNR to be used for service discovery in ad hoc networks, since it preserves protocol reliability while significantly reducing the number of transmissions for service discovery, and so the power consumed.

4 Proposed Improvements to Multicast DNS

As we have seen above, Multicast DNS is more efficient for service discovery in ad hoc networks than LLMNR. However, the traffic efficiency of the protocol can be

significantly improved with some simple modifications. In this section we propose four simple modifications, and evaluate how they improve the performance of Multicast DNS. They all try to reduce the number of network transmissions and receptions, particularly for the more limited devices, and so their power consumption.

4.1 Use Services Stored in the Cache for the Answers

In ad hoc networks, cooperation among devices is essential since the devices can carry out more complex tasks at a lower cost thanks to the cooperation. Our first proposal of modification for Multicast DNS is to allow all the devices that know about a service, not just those devices that offer themselves the service, to answer a service request query. In other words, we allow using the resource records in the cache (i.e., the non-authoritative resource records) for the replies.

Moreover, prior to answering, a device first listens for answer messages to the same query from other devices[2], it checks whether it knows about any other service that has not been announced yet, and if so, it sends its answer message, and if not it aborts its reply. This way, all devices cooperate to build the list of all available services of the requested type with the minimum number of messages transmitted, see Figure 3. In this figure, we can see that the reduction in the number of messages transmitted in this scenario is $12,4\%$ for big enough caches.

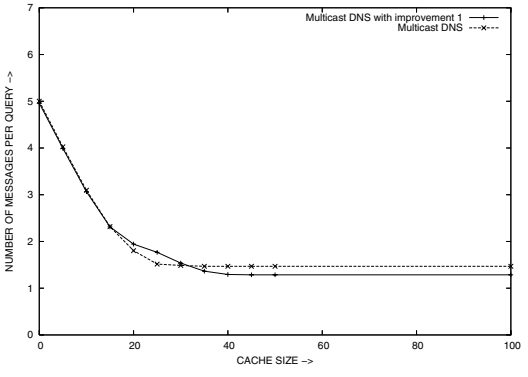


Fig. 3. Number of messages against cache size with improvement 1

4.2 Update the Cache with the Services Included in the Query

Continuing with the philosophy of exploiting the cooperation between devices, the second improvement we propose consists on updating the caches not just with the resource records obtained from answer messages, as Multicast DNS specifies, but also from the list of previously known services included in search queries. This way, as Figure 4 shows, the number of search messages is reduced in our scenario a $22,8\%$ with respect to Multicast DNS, for big enough caches.

[2] Remember that, to avoid collisions, in Multicast DNS all devices wait a random time before sending a reply to a query. We will come back on this later in this section.

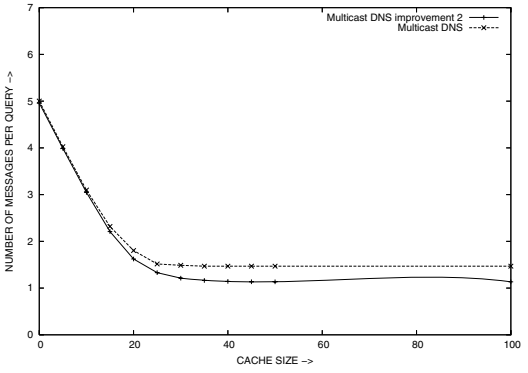


Fig. 4. Number of messages against cache size with improvement 2

4.3 Use a Different Distribution for the Random Waiting Time

In Multicast DNS, to avoid collisions after a query, servers do not answer immediately, but wait a random time drawn from a uniform distribution between 20 and 120 msec. Our third proposal consists on generating this random time following a more intelligent distribution that statistically guarantees that devices with less energy constraints (e.g., with an AC adapter plugged in), and which know about more services, answer first, making most of the times unnecessary for the most limited devices to answer. To achieve this, we propose to generate the random time inversely proportional to the Time-To-Live (TTL) associated to the device, and to the number of services it knows. We assume that battery powered devices will have a low TTL configured (which is consistent with the fact that they are highly mobile).

Specifically, we propose the random time to be drawn from the expression in Equation 2, where $U(x, y)$ represents a uniform distribution between x and y, and the value 7200 sec. (120 minutes) is an heuristically chosen parameter that represents the time starting from which a device can be considered static.

$$\mathrm{U}(20, \quad 120 * \frac{7200}{7200 + \mathrm{TTL} * \#\mathrm{Cache\_Entries}}) \tag{2}$$

We have simulated an example scenario to measure what percentage of the answer messages are transmitted by different devices with different TTL values, in a heterogeneous scenario with 20 devices in average, with five different values of TTL: 500, 2500, 4500, 6500 and 9500 seconds, which are also their average thinking times. There are the same number of devices of each type (i.e., 20% with each TTL). The cache has a capacity for 10 entries, except for the more static devices (the ones with TTL = 9500), that are less limited and have a cache with capacity for 100 entries. The rest of the parameters of the simulation are the same than in previous ones.

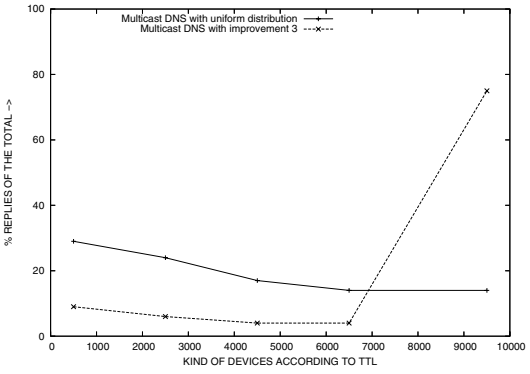


Fig. 5. Percentage of answer messages against TTL of the device with improvement 3

Figure 5 shows the results of this simulation. We see that changing the strategy of generation of the random waiting time causes that 75% of the queries are answered by the devices with larger TTL, reducing the answer messages from the others to a forth of what they would have answered with an uniform distribution (as in Multicast DNS), and so reducing their power consumption. Moreover, the number of messages sent is reduced a $58,86\%$ because the devices with larger TTL and greater cache, which answer the 75% of the queries, are the ones that have a more complete and accurate view of the network, and most of the times the reply from any other device is not needed because there is no other new service to add.

4.4 Optimize "One Query-One Response" Queries

As we observed before, Multicast DNS distinguishes three modes of operation of the applications in search for a service: "one-shot queries" (also known as "one query-one response"), one-shot queries accumulating multiple responses ("one query-multiple responses"), and continuous querying. However, no field in the DNS message is used to distinguish one type of query from the other, and so the answers from the servers are the same in all cases; it is the client itself which, for example, in the case of one-shot queries, selects the first answer and discards the rest.

Our last proposal consists on defining a flag in the DNS header that could be used in Multicast DNS to indicate whether the query is of the kind "one query-one response" or "one query-multiple responses". For this flag, any of the currently unused bits (9 to 11) of the parameters field of the DNS message header could be used.

This way, if a server receives a DNS query with the "one query-one response" flag set, before sending its reply, if it listens another reply from other device in the network, it will abort its reply, even though it would have something new to say. This way, the bandwidth consumed is greatly reduced.

5 Conclusions and Future Work

In ad hoc networks, devices must be able to discover and share services dynamically. Several protocols have been proposed for service discovery. Recently the IETF has proposed the use of the DNS protocol for service discovery. For ad hoc networks, the IETF works in two proposals of distributed DNS, that can be used for service discovery: Multicast DNS and LLMNR.

In this paper we have reviewed and analyzed both proposals from the point of view of their efficiency when used for service discovery in ad hoc networks. From our study, we conclude that the one that better fits the requirements of these kinds on environments is Multicast DNS. However, some very simple improvements can be introduced that help to improve their efficiency, especially regarding power consumption in limited devices. In this paper we have proposed and analyzed through simulation four improvements. The reduction in the number of messages transmitted is about 35%, depending on the scenario, for one query-multiple response requests, and may be much greater for one query-one response. Besides, this reduction is achieved in those devices where it is more necessary, in the more limited devices.

We are working on validating the viability of our proposals via real implementation. In this sense, starting from an implementation in J2SE of Bonjour [19], we are completing an implementation in J2SE of Multicast DNS and DNS-SD with and without the power-saving improvements we propose. There is also an implementation of Rendezvous for network cameras Axis 2100.

As a future work, besides finishing the implementation of our improvements to Multicast DNS in J2ME for PDAs, and in other devices usually found in pervasive computing environments, we are also interested in broaching the following problems. First, we want to test other distributions for the generation of the random time, and to study their effect and how to achieve a further reduction. Secondly, today the value of TTL is configured manually both in Multicast DNS and in LLMNR devices, but it would be very interesting that this value could be automatically learned from the mobility behaviour of the device, without any direct intervention from the user. Thirdly, we plan to do more simulations using different multicast ad-hoc routing protocols in larger areas, instead of IP broadcasts. Finally, we are aware of the security problems inherent with ad hoc networks, and we are working in a distributed trust model, so these networks can include automatic mechanisms to adapt the trust relation between the devices as they experiment positive and negative experiences [20].

References

1. RFC 2165: Service Location Protocol (1997)
2. Goland, Y.Y., Cai, T., Leach, P., Gu, Y.: Simple Service Discovery Protocol/1.0. Internet-Draft (work in progress) (1999) draft-cai-ssdp-v1-03.txt.
3. Jini: Architectural Overview. White Paper (1999)
4. Salutation Consortium: Online available at http://www.salutation.org (1998)
5. Bluetooth: (Specification v1.1, Part E: Service Discovery Protocol (SDP))

6. Association, I.D.: Infrared data association link management 1.1 (1996)
7. Chakraborty, D., Joshi, A., Yesha, Y., Fini, T.: GSD: A Novel Group-based Service Discovery Protocol for MANETS. In: 4th IEEE Conference on Mobile and Wireless Communications Networks (MWCN 2002), Stockholm. Sweden (2002) 140–144
8. Oh, C.S., Ko, Y.B., Kim, J.H.: A Hybrid Service Discovery for Improving Robustness in Mobile Ad Hoc Networks. In: The International Conference on Dependable Systems and Networks. DSN-2004, Florence, Italy (2004)
9. Nidd, M.: Service Discovery in DEAPspace. IEEE Personal Communications (2001)
10. Helal, S., Desai, N., Verma, V., Arslan, B.: Konark: A System and Protocols for Device Independent, Peer-to-Peer Discovery and Delivery of Mobile Services. IEEE Transactions on Systems, Man, and Cybernetics **33**(6) (2003) 682–696
11. Barbeau, M., Kranakis, E.: Modeling and Performance Analysis of Service Discovery Strategies in Ad Hoc Networks. In: International Conference on Wireless Networks. ICWN 2003, Nevada. Canada (2003) 44–50
12. Campo, C., Garcia-Rubio, C., Marin, A., Almenarez, F.: PDP: A lightweight discovery protocol for local-scope interactions in wireless ad hoc networks. Computer Networks (2006)
13. Zhu, F., Mutka, M., Ni, L.: Service discovery in pervasive computing environments. IEEE Pervasive Computing (2005)
14. Jones, C.E., Sivalingam, K.M., Agrawal, P., Chen, J.C.: A Survey of Energy Efficient Network Protocols for Wireless Networks. Wireless Networks **7**(4) (2001) 343–358
15. Feeney, L.M., Nilsson, M.: Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment. In: IEEE INFOCOM. (2001)
16. Cheshire, S., Krochmal, M.: DNS-Based Service Discovery. Internet-Draft (work in progress) (2005)
17. Cheshire, S., Krochmal, M.: Performing DNS queries via IP Multicast. Internet-Draft (work in progress) (2005)
18. Esibov, L., Adoba, B., Thaler, D.: Linklocal Multicast Name Resolution (LLMNR). Internet-Draft (work in progress) (2005)
19. http://jmdns.sourceforge.net/.
20. Díaz, D., Marín, A., Almenárez, F.: A smartcard solution for access control and trust management for nomadic users. In: Seventh Smart Card Research and Advanced Application IFIP Conference (CARDIS 2006), Tarragona (Spain) (2006)

A Hop-by-Hop Multipath Routing Protocol Using Residual Bandwidth for Wireless Mesh Networks

Eun-Joo Oh, Sungil Lee, and Jae-Sung Lim

Graduate School of Information and Communications, Ajou University
San 5, Wonchun-dong, Youngtong-gu, Suwon, 447749, South Korea
{oezoo, openlsi, jaslim}@ajou.ac.kr

Abstract. In wireless mesh networks, there are mesh routers which can compose a wireless backbone with low mobility. We propose a hop-by-hop multipath routing scheme which is suitable for mesh routers offering network reliability with route redundancy. We extend DSDV in order to have multiple next hops to all nodes in the network without additional overheads. The basic idea of our scheme is to make several paths between the source and destination by selecting a proper next hop at every forwarding data. We choose a mesh router with the highest residual bandwidth as a next hop among multiple ones. Through periodic one hop broadcasting, not only we can get residual bandwidth information but also we can detect route failures fast and reduce the number of routing overhead packets. Through simulation, we represent that our scheme is more efficient than DSDV in delivering data to the destination when traffic is heavy, reducing overhead packets in the network, and preventing data loss when the route failure occurs.

Keyword: Wireless mesh networks, Routing, Proactive routing, Hop-by-Hop multipath, Residual bandwidth.

1 Introduction

As the use of Internet is increased, the demand to utilize Internet wherever and whenever is also increased. Because the size of devices is getting smaller and the capacity of them is getting better, they can satisfy the increasing demand for Internet. In these points of view, wireless mesh networks come. Wireless mesh networks take charge of connections both between the same networks and among the different networks. This fact makes it possible to use any data located in Internet or other networks whenever people want to. Wireless mesh networks consist of mesh routers and mesh clients. Mesh routers act as bridges which connect to different networks, gateways which connect to the Internet, and a wireless backbone. Mesh clients, as wireless terminals, can be hosts and routers like nodes in Ad-Hoc networks. Mesh clients also perform as a ad hoc gateway in order to connect to the wireless mesh backbone to access Internet[1].

We find out that mesh routers have similar characteristics to the nodes in Ad-Hoc networks such as wireless multi-hop communication. However, the mesh routers have

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 123 – 134, 2006.

different features in that they have very low mobility and no energy constraint, and they form a wireless infrastructure backbone including the bridging and gateways functions. The main data in wireless mesh networks must be the data from or to Internet through gateways. Moreover, it is expected that there are a lot of data traffics among mesh routers, especially audio and video traffics which are sensitive of a time and should satisfy QoS(Quality of Service) requirement. Therefore, a new routing protocol is necessary among mesh routers to reflect these unique characteristics and it should be different from the existing routing protocols in Ad-Hoc networks.

A lot of routing protocols has been studied in Ad-Hoc networks actively[2]-[9]. Routing is a very challenging task in Ad-Hoc networks because the Ad-Hoc networks have characteristics such as the unpredictability of environment due to node failure, the unreliability of wireless medium, resource-constrained nodes, and dynamic topology due to mobility. Ad-Hoc routing protocols are divided largely into two parts according to the time when a routing path is determined. The routing path is calculated whether before or at transmitting data, which are proactive protocols (DSDV[4], OLSR[5]) and reactive protocols(DSR[6], AODV[7]). The proactive protocols are also called table-driven schemes and they calculate the routing path before transmitting data. Each node in the network exchanges its routing table periodically and it can know network information such as the topology, the link state, and the routes. After setting up the routing table, the nodes can know the path to all nodes in the network and they can send data immediately whenever data to send is occurred. The reactive protocols are also called on-demand schemes and they calculate the routing path at transmitting data. Because these schemes calculate the path to the destination only when data to send is occurred, they don't have to exchange the routing tables periodically. They can reduce the number of overhead packets but the end-to-end delay is increased because data are able to be sent after calculating the routing path[2], [3].

In Ad-Hoc networks, DSDV[4] is a renowned proactive routing protocol. As a distance vector scheme, DSDV selects a next hop which has minimum hop counts to the destination. By exchanging routing tables, each node in the network can know the distance information as hop counts and next hops for all other nodes in the network with the minimum distance. As a proactive routing scheme, DSDV updates the routing table periodically. There are two ways to update the routing table, one, called a full dump, will carry all of the available routing information. The other, called an incremental, will carry only information changed since the last full dump. When the routing table is updated, routes are always preferred if the sequence numbers are newer and if the sequence numbers are the same and yet the lower hop count is better. The sequence number prevents the formation of loop because the route which has newer sequence number is preferred.

To compensate for the dynamic and unpredictable nature of Ad-Hoc networks, multipath routings are studied actively, too[9]. Multipath routing allows the establishment of multiple paths between a single source and single destination node. Load balancing can be achieved by spreading the traffic along multiple routes. If multiple paths are used simultaneously to route data, the aggregate bandwidth of the paths may satisfy the bandwidth requirement of the application. Since there is more bandwidth available, smaller end-to-end delay may be achieved. In [10], it is showed

that a distance vector routing could be extended to offer the computation of all possible alternative paths with instance loop freedom.

Proactive routing protocols are proper for wireless mesh networks especially among mesh routers due to the mesh routers' characteristics. As a wireless backbone, the traffic patterns of mesh routers are likely that a large subset of nodes communicate with each other and the source and destination pairs are also changing with time. If mesh routers know all network information, they can minimize end-to-end delay by sending data without calculating a path to destination. In multi-hop wireless networks, as hop counts to traverse increase, the throughput is sharply decreased. This has been confirmed by several simulation studies based on 802.11 and other MAC(Medium Access Control) protocols similar to 802.11[12], [13]. We prefer DSDV because it is one of the well-known proactive routings and selects a next hop with minimum hop counts to the destination. However, it is hard to offer networks route redundancy for reliable data transmission because DSDV maintains just one next hop to each destination. Generating a lot of routing overhead packets is also a weak point of the proactive routing schemes to declare and update routing tables. If the data transmitting route gets into trouble, DSDV takes much time to recover the route and causes a lot of data loss. QoS metrics such as the bandwidth, the link state, and the queue state are hard to apply to DSDV because it is difficult to come up with network's information changed rapidly through periodic routing table updates.

In this paper, we propose the hop-by-hop multipath scheme of extending DSDV and adding a neighbor table containing residual bandwidth information. By extending DSDV, mesh routers can get multiple next hops without any additional packets or calculations. The multiple next hops should have minimum hop counts to all destinations. They enable our proposed scheme to operate as the hop-by-hop multipath based on minimum distance. Mesh routers make and maintain a neighbor mesh routers' table by using a HELLO message containing residual bandwidth information. We calculate the residual bandwidth according to [11] using HELLO bandwidth estimation. When a mesh router transmits data, it selects one of the multiple next hops according to the residual bandwidth information in the neighbor table, larger bandwidth value is preferred. Through the periodic broadcasting of HELLO messages, mesh routers can detect the state of topology fast. If the mesh router does not take periodic HELLO messages from neighbor routers, it concludes that the neighbor router has problem and it changes the next hop with another one to the destination directly without any additional procedure. The HELLO message also can make routing table updates operated only when there is no route to the destination. Our proposed scheme can deliver a lot of data to the destination by distributing data to the network using multiple next hops and residual bandwidth information especially when the data traffic is heavy. It can also reduce the number of routing overhead packets by modifying the routing update scheme of DSDV with the neighbor table, and prevent a lot of data loss by detecting problem quickly and changing a next hop directly.

This paper is organized as follows: In Section 2, we introduce our proposed routing scheme. In Section 3, we represent our simulations and discuss the performance results obtained from a series of simulations. In Section 4, we will make conclusions and future research.

2 Proposed Scheme: HMP Routing Protocol

In this paper, we propose a new routing protocol suitable for mesh routers. We call the proposed scheme HMP(Hop-by-hop MultiPath) routing protocol. The HMP has two routing tables: a forwarding table and a neighbor table. The forwarding table is a routing table similar to DSDV's but it has multiple next hop information to all the other mesh routers in the network with minimum hop counts. The neighbor table is a table which stores neighbor routers' residual bandwidth information and it is used to choose a next hop and come up with the change of network state.

2.1 Forwarding Table: Multiple Next Hops

We modify DSDV because it has relatively little overhead among proactive routing protocols and it is simple to be extended to a multipath scheme. We represent a new approach to add a multipath capability to DSDV. We modify DSDV's routing table in order to take multiple next hop information to the destination with minimum hop counts. The basic idea of our scheme is to make several paths between a source and destination by selecting a proper next hop among multiple ones at every forwarding data, as a hop-by-hop multipath scheme.

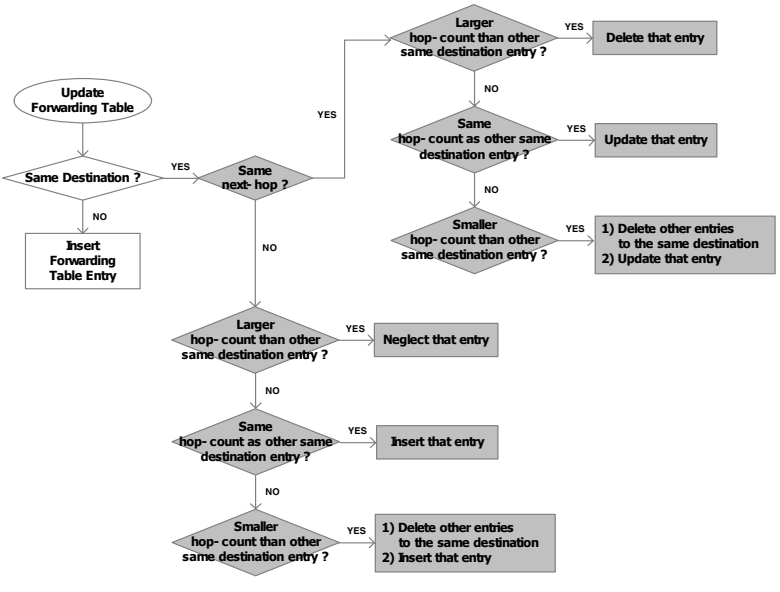


Fig. 1. Procedure of Forwarding Table Update

Figure 1 shows the way of modifying the procedure of DSDV to get multiple next hop information to all nodes in the network without any additional routing overheads. When exchanging routing tables, if the received updating message has the same sequence number but it is from a different mesh router, the message is used to update a forwarding table. Even though the incoming information has the same destination, it

is determined whether to be used or not according to the next hop information. This way gives multiple next hops to the routing table. After checking the next hop information, it checks hop counts. According to the hop counts, the update procedure is changed as shown in figure 1. This way makes the routing table get the minimum hop counts to the all destinations. Without any additional routing messages or calculations, we can get the forwarding table containing multiple next hops to all mesh routers with the minimum hop counts.

Our proposed multipath scheme can distribute data all over the network and achieve the load balancing using next hops properly. This distributing feature can prevent the occurrence of bottleneck mesh routers, especially when the amount of data is increased all over the network. Therefore, our scheme improves the efficiency of data delivery. Our proposed scheme can also improve the reliability of data transmission with route redundancy. When a mesh router in the route gets some problem such as link or route failures, one of other next hops can be used immediately without any other procedure to recover the route. Therefore, our proposed scheme decreases a lot of data loss when the route has problem.

Once forming topology among the mesh routers, the topology is hardly changed due to low mobility and the routing table's information can be used for relatively long. Therefore, the periodic routing table update in DSDV is not quite necessary. We modify the routing table update so that the update is performed only when a new mesh router joins or leaves the network. Even though the topology is changed, we can delay the routing table update until there is no route to the destination in order to reduce overhead packets more. Because our proposed scheme has multiple routes to the destination, the routing tables are updated only when there is no route to the destination. This modification can reduce a great number of routing overhead packets.

2.2 Neighbor Table: Residual Bandwidth and Topology Control

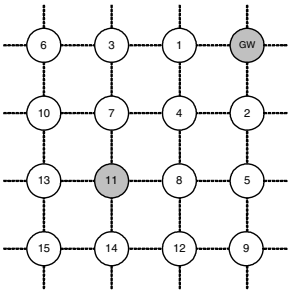
We propose making a neighbor table through HELLO messages to store residual bandwidth information of neighbor mesh routers and control topology. The HELLO message contains residual bandwidth information and it is exchanged between one-hop neighbor routers through a periodic broadcasting. Being different from the forwarding table, the neighbor table maintains the information of just one hop neighbor. The information of the neighbor table is used to select a next hop out of multiple next hops when transmitting data. The mesh router with the maximum residual bandwidth is selected as a next hop. This means that we select a path with higher bandwidth among several paths keeping minimum hop counts.

We calculate the residual bandwidth according to [11] as the raw link capacity minus the overall consumed bandwidth, divided by a weight factor. It is necessary to divide the residual bandwidth by the weight factor due to IEEE 802.11 MAC's nature which RTS(Request To Send), CTS(Clear To Send), and ACK(ACKnowledgement) packets consume bandwidth, the back-off scheme cannot fully use the entire bandwidth, and packets can collide, resulting in packet retransmissions. Each mesh router broadcasts its residual bandwidth information periodically calculating through above method. We think that if a mesh router has more residual bandwidth, the router has more ability to manage data efficiently and the data can be transmitted with higher transmission rate. Therefore, selecting a next hop which has a maximum

residual bandwidth basically minimum hop counts helps the network use the capacity of 802.11 WLAN(Wireless Local Area Network) evenly, reduce waste of network bandwidth due to reducing retransmission, distribute data to the router with more data processing capacity, and prevent a network from occurring bottleneck mesh routers.

We can use the neighbor table to control topology by finding out the routers' state. The neighbor table also makes it possible to update the forwarding table only when the network topology is changed. If neighbor router's information is not updated for a certain time, we can conclude that the mesh router already leaved the network or the router has a problem. Then, the router sets the residual bandwidth of the neighbor router zero in order not to select the router as a next hop. It can send data through another next hop directly. If the residual bandwidth of all possible next hops is zero, which means that there is no route to get to the destination, the forwarding table update is started through all over the network. At this moment, the entries that have zero residual bandwidth in the neighbor table are deleted. This method reduces the amount of data loss by using another next hop directly and it can also reduce the number of routing overhead packets not by updating routing tables immediately and periodically all over the network.

The interval of broadcasting HELLO messages is thoroughly related to the time to know a route failure and a topology change. If the interval is short, the time to detect a route failure is also short but the number of overhead packets is increased. On the other hand, if the interval is long, the time to detect a route failure is also long but the number of overhead packets is decreased.



(a) Example Topology of 4x4 Grid

Neighbor Table of 11		
Nghr.	R_BW_	...
7	5 M	...
8	10 M	...
13	8 M	...
14	8 M	...

(c) Neighbor Table

Forwarding Table of 11			
Dst.	Nxt_Hp	Hp_Cnt	...
GW	7	4	...
	8	4	...
1	7	3	...
	8	3	...
2	7	3	...
	8	3	...
3	7	2	...
4	7	2	...
	8	2	...
5	8	2	...
6	7	3	...
	13	3	...
7	7	1	...
8	8	1	...
9	8	3	...
	14	3	...
10	7	2	...
	13	2	...
11	0	0	...
12	8	2	...
	14	2	...
13	13	1	...
14	14	1	...
15	13	2	...
	14	2	...

(b) Forwarding Table

Fig. 2. Example Tables of Proposed Scheme

Figure 2 shows an example of a forwarding table and a neighbor table as a result of operating the proposed scheme in 4x4 grid topology. Let's assume that the router 11 wants to send data to the GW. First, the router 11 sees the forwarding table to find a next-hop. Next, the router 11 can know there are two next hop candidates, router 7 and 8. Then, the router 11 sees the neighbor table to determine which next hop has more residual bandwidth. Finally, the router 11 chooses the router 8 as a next hop and sends data through the router 8. In case that the router 8 leaves the network, the router 11 can not take the HELLO message from router 8. The router 11 sets the residual bandwidths of router 8 zero in the neighbor table. Then, the router 11 sends data to the GW through the router 7. Because the residual bandwidths of the router 8 become zero the router 11 does not choose the router 8 as a next hop.

3 Simulations

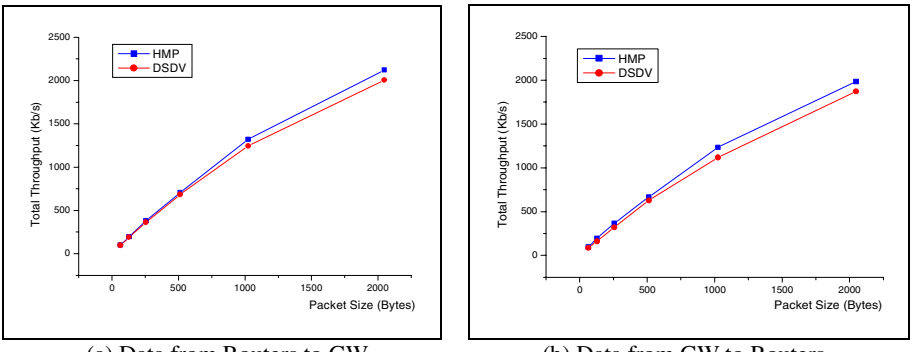
We evaluated the proposed scheme through NS-2. The simulation was conducted with the following parameters. The simulation topology is the same as figure 2(a).

Table 1. Simulation Parameters

Parameter	Value
Topology	4x4 grid topology
The number of nodes	16
Distance between nodes	50 m
Transmission range	50 m
Traffic	FTP
Packet size	64 ~ 2048 bytes
MAC protocol	802.11 WLAN
Link bandwidth	11 Mbps
The broadcasting interval of HELLO message	10 seconds
Simulation time	200 ~ 300 seconds

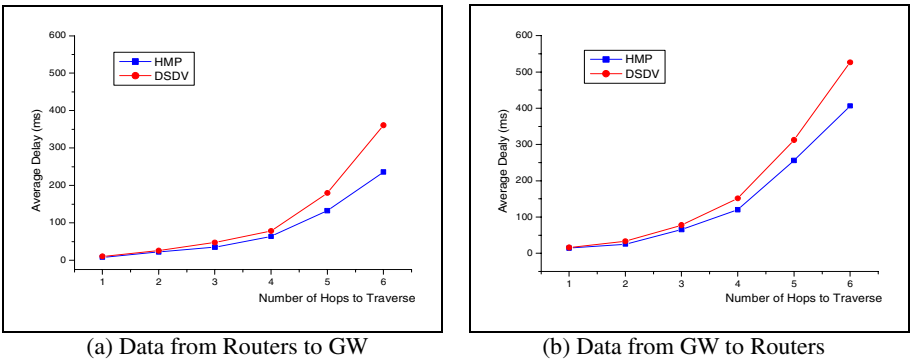
Figure 3 shows the total throughput with increase of the packet size. Figure 4 shows the average delay according to the number hops to traverse when the size of packet is 1024 bytes. In the simulation of figure 3 and 4, routers 2, 3, 8, 10, 14, 15, and GW participate in data communication showed in figure 2(a). The packet size is increased with the following 64, 128, 256, 512, 1024, and 2048 bytes.

We can see that HMP shows better performance of throughput and delay than DSDV in all cases in figure 3 and 4. As the size of packet increases, the throughput gap between HMP and DSDV gets wide. Similarly, as the hop counts to traverse increases, the delay gap between HMP and DSDV gets wide, too. The reason why HMP has better performance is that HMP can distribute data to the networks evenly using multiple next hops properly based on the residual bandwidth information. HMP achieve better performance of the total throughput and the average delay when there are a lot of data in the network.



(a) Data from Routers to GW (b) Data from GW to Routers

Fig. 3. Total Throughput with Packet Size



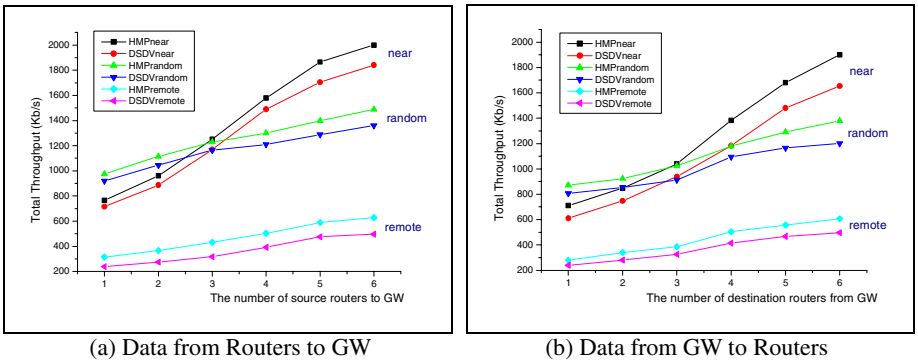
(a) Data from Routers to GW (b) Data from GW to Routers

Fig. 4. Average Delay with the Number of Hops

In figure 3, the total throughput of both HMP and DSDV increases as the size of packet is increased, but the rate of increase becomes slow. In figure 4, the average delay of both HMP and DSDV increases sharply as the hop count to traverse is increased. As the hop count to traverse is increased, the data experience more contentions in MAC layer. Therefore, we can observe that the average delay increase sharply according to the hop counts in the figure 4. Especially, the amount of data in the network is increased, the contention becomes severe. Moreover, as the amount of dada is increased in the network, each router's queue is filled with data to send or retransmit. Therefore, the total throughput is saturated showed in the figure 3.

Figure 5 shows the total throughput according to the location and the number of mesh routers which participate in transmitting data when the size of packet is 1024 bytes. The sources or destinations are selected according to the following rules. First, remote routers from the GW are selected(from router 15 to router 10). Next, the mesh routers are randomly selected(from router 1 to router 15). If the randomly chosen router finishes the data transmission, the other router is randomly chosen to send data during randomly chosen transmission time to the destination. Finally, near routers to the GW are selected(from router 6 to router 1).

We can see that HMP shows better throughput than DSDV in all cases. As the number of source or destination routers increases, the throughput gap between HMP and DSDV gets wide. We observe that the sources or destinations which are located close to the destination or source have better throughput in the figure 5. As the distance between the source and destination is increased, the throughput is decreased. The reason why HMP shows better performance is the same as we explained early in previous figures, figure 3 and 4.



(a) Data from Routers to GW (b) Data from GW to Routers

Fig. 5. Total Throughput with Location and the Number of Routers

We can consider the hop counts from the GW as a mesh router's location. The location considerably affects network performance showed in figure 4 and 5 due to the nature of IEEE 802.11 MAC such as RTS, CTS, and ACK. The difference of throughput and delay according to the location is very large and this fact gives rise to unfairness and difficulty of the performance in order to support time-sensitive data. Therefore, the ways to guarantee QoS and fairness are necessary and very important. We will take into account these issues in the future.

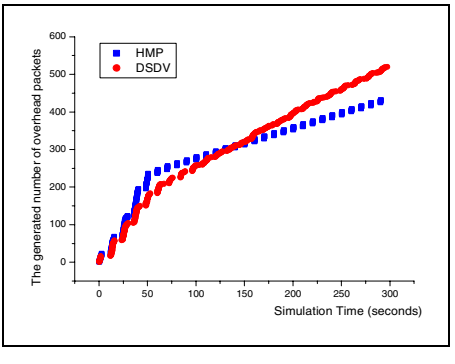


Fig. 6. Generated Overhead Packets

Figure 6 shows the generated overhead packets in the network. Because DSDV and HMP exchange routing tables before sending data, they generate lots of overhead

packets at the beginning of simulation. However, as the simulation time increases, the overhead packets of DSDV and HMP are not increased sharply. Compared with DSDV, HMP generates more overhead packets at the beginning of simulation but it generates fewer overhead packets than DSDV with increase of the simulation time. This is because HMP generates routing table update packets and neighbor table update packets simultaneously at the beginning of simulation. However, HMP does not generate overhead packets for periodic routing table updates after getting network topology as long as the topology is not changed. After getting network topology, HMP exchanges only HELLO messages. Therefore, the rate of generating overhead packets of HMP becomes very slow.

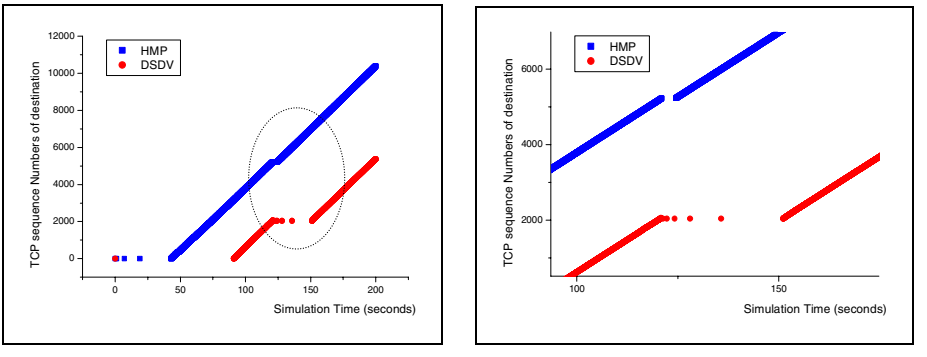


Fig. 7. Sequence Numbers of TCP

Figure 7 shows the sequence numbers of TCP in the destination. In this simulation, there are one source(router 15) and one destination(GW). The source sends data consecutively and when it arrives 120 second, the route is failed. The right figure is the magnified version of the left one around 120 second. In the figure 7, HMP starts transmitting data faster than DSDV because HMP takes less time to know network information by modifying the routing table update scheme. Because DSDV meets several periodic routing table updates during initial forming a forwarding table, DSDV takes more time to construct a forwarding table.

After the route failure, each routing protocol detects the route failure and operates each procedure of route repairs. When a route failure is occurred, DSDV operates periodic forwarding table updates without any procedure of detection or repair. DSDV takes about 30 seconds to recover the route in the simulation, which can be identified through breaking sequence number of DSDV. When a route failure is detected through HELLO message, HMP doesn't have to update the forwarding table immediately. HMP operates the neighbor table update by setting the failed router's residual bandwidth zero and did not choose the failed router as a next hop as we proposed. HMP can be aware of the route break faster than DSDV depending on the interval of broadcasting residual bandwidth information and HMP find another path directly to the destination. In our simulation, HMP takes about 5 seconds to restart transmitting data and it detects the route failure within the maximum 10 seconds. Therefore, HMP can reduce a lot of data loss by finding and using another path to the

destination fast and directly with multiple next hop information and the periodic HELLO message when route break is occurred.

4 Conclusions and Future Research

We have proposed a new hop-by-hop multipath routing scheme that is suitable for mesh routers in wireless mesh network by extending DSDV and adding the exchange of HELLO message. The proposed HMP routing protocol has two routing tables. One is a forwarding table containing multiple next hop information with minimum hop counts which makes possible to be hop-by-hop multipath. The other is a neighbor table with the neighbor routers' residual bandwidth information to determine a next hop and control the topology. Our scheme has better reliability to transmit data and it can distribute data over the network with preventing bottleneck. Through simulations by NS-2, we represented that our scheme is better than DSDV in delivering data efficiently when traffic is heavy, reducing the amount of overhead, and transmitting data when the route failure is occurred.

We represented that the performance of throughout and delay decreases sharply according to the location and the amount of traffic due to the nature of IEEE 802.11 MAC. Therefore, the ways to guarantee QoS and fairness are necessary and very important and we will extend our proposed scheme so as to provide QoS and fairness support. In this paper, we considered only mesh routers which have very low mobility in a static topology but, in the future, we will take into account the mobility of mesh routers and mesh clients in dynamic topology. Our proposed scheme is not guaranteed to be the best choice because the selected neighbor's neighbor may have very little available bandwidth. We will discuss this problem more and try to solve it. We will consider extending OLSR to a multipath scheme for wireless mesh networks.

References

1. I. F. Akyildiz, X. Wang, and W. Wang, ``Wireless Mesh Networks: A Survey" Computer Networks Journal (Elsevier), vol. 47, pp. 445-487, Mar. 2005.
2. E. M. Royer and C. K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, vol. 6, pp. 46-55, Apr.1999.
3. X. Zou, B. Ramamurthy, and S. Magliveras "Routing Techniques in Wireless Ad Hoc Networks - Classification and Comparison", The Sixth World Multiconference on Systemics, Cybernetics, and Informatics (SCI '02), vol. 4, Jul. 2002
4. C. E. Perkins and P. Bhagwat "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", ACM Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94), pp.234-244, Aug. 1994
5. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol for Ad Hoc Networks", Proceedings of IEEE International Multi Topic Conference (INMIC '02), pp. 62-68, Dec. 2002
6. DSR – D. B. Johnson, D. A. Maltz, and Y. C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks(DSR)", Internet Draft, Apr. 2003
7. AODV – C. E. Perkins and E. M. Royer, "Ad hoc On-demand Distance Vector(AODV) Routing", In Proceeding of Second IEEE Workshop on Mobile Computing System and Application (WMCSA '99), pp. 90-100, Feb. 1999.

8. R. Jansen, S. Hanemann, and B. Freisleben, “Bandwidth Efficient Distance Vector Routing for Ad Hoc Networks”, In Proceedings of the Wireless and Optical Communications Conference (WOC ‘01), pp. 117-122, Jun. 2001.
9. S. Mueller, R. P. Tsang, and D. Ghosal, “Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges”, Lecture Notes in Computer Science, vol. 2965, pp. 209 – 234, Apr. 2004.
10. S. Vutukury and J.J. Garcia-Luna-Aceves, “MDVA:A Distance-vector Multipath Routing Protocol”, In Proceeding of IEEE INFOCOM (INFOCOM ’01), vol. 1, pp. 557-564, Apr. 2001.
11. L. Chen and W. B. Heinzelman, "QoS-aware Routing Based on Bandwidth Estimation for Mobile Ad Hoc Networks", IEEE Journal on Selected Area in Communications (JSAC ‘05), vol. 23, pp. 561-572, Mar. 2005.
12. M. Gerla, R. Bagrodia, L. Zhang, K. Tang, and L. Wang, “TCP over Wireless Multi-hop Protocols: Simulation and Experiments”, In Proceeding of IEE International Conference on Communications (ICC ’99), Jun 1999.
13. G. Holland and N. Vaidya, “Analysis of TCP Performance over Mobile Ad Hoc Networks”, In proceeding of ACM Conference of Mobile Communication (MOBICOM ’99), Aug. 1999.

Lowest Weight: Reactive Clustering Algorithm for Adhoc Networks

Mohamed Elhoucine Elhdhili, Lamia Ben Azzouz, and Farouk Kamoun

CRISTAL, Ecole Nationale des Sciences de l'Informatique, University of Manouba Tunisia
Mohamed.Elhdhili@cristal.rnu.tn,
{Lamia.Benazzouz, Farouk.Kamoun}@ensi.rnu.tn

Abstract. In this paper, we address clustering in ad hoc networks. Ad hoc networks are a wireless networking paradigm in which mobile hosts rely on each other to keep the network connected without the help of any pre-existing infrastructure or central administrator. Thus, additional features pertinent to this type of networks appeared. In fact, centralized solutions are generally inadaptable due to the need for cooperative network operations. To ensure efficient, tolerant and durable cooperative operations, nodes need to organize themselves. Clustering is an organization method which consists in grouping the nodes into clusters (groups) managed by nodes called clusterheads. In this paper, we present existing clustering algorithms and propose a new solution inspired from two of these algorithms (Lowest Id and WCA). This solution, called Lowest Weight, exploits their advantages and relieve to their drawbacks in terms of clusters stability and computational overhead. Simulation experiments were conducted to evaluate the performance of the algorithm proposed in terms of clusters numbers, clusterheads lifetime and the number of reaffiliations (node moving from a cluster to another). Results show that Lowest Weight ameliorate performs of existing algorithms especially regarding mobility leading to more suitable, adaptable, scalable and autonomous clustering.

1 Introduction

An ad hoc network is a multihop wireless network supporting cooperative mobile nodes without any existing infrastructure. In this type of networks, management tasks must be distributed over all nodes. Clustering might be an interesting technique for ad hoc networks to ensure efficiently these management tasks such as routing, addressing, transmission management and security. It consists in dividing the network into clusters managed by nodes called clusterheads. However, this technique can lead to the clusterheads congestion (processing, routing...etc). In addition, signalling messages used for executing the clustering algorithm and updating clusters can degrade the network performances. An efficient clustering algorithm must adapt itself to frequently and unpredictable topology changes known in ad hoc networks. It must also generate stable clusters as much as possible to prohibit their updates which can lead to update other information as routing, security, addressing and management information [1, 2].

In the literature, different works proposed clustering algorithms for ad hoc networks. These algorithms have different purposes (routing efficiency, transmission

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 135 – 146, 2006.

management, backbone formation…etc.). Our works are inspired from two existing clustering algorithms called Lowest Id [3, 4] and WCA: Weighted Clustering Algorithm [5], to propose an algorithm (Lowest Weight) that combines their strength and relieve to their limits.

WCA has the advantage of electing clusterheads based on a weight related to energy consumption, mobility, distance to neighbours and connectivity degree. However, it has drawbacks in the strategy used to divide the network into clusters since it uses a great number of clustering messages (broadcasting, many times, clustering messages in the whole network). Lowest Id minimizes this number because each node broadcasts clustering messages once and only to its one-hop neighbours. But, it uses a non suitable metric (the node identification).

The rest of the paper is organized as follows: in section 2, we present existing clustering algorithms underlying their advantages and limits. In section 3, we describe the proposed clustering algorithm. Section 4 discusses the robustness and efficiency of our solution in comparison with existing ones. Section 5 presents simulations conducted to evaluate the performances of our algorithm. The conclusion outlines our immediate future work.

2 State of the Art

Many works have recently proposed clustering algorithms for ad hoc networks [3-9]. These works present advantages but some drawbacks as a high computational overhead for both clustering algorithm execution and update operations. We can classify these algorithms into two main categories: proactive algorithms and reactive ones. Most of them are proactive. Only WCA [5] is reactive. In this section, we present, in a first stage, the proactive group highlighting their advantages and drawbacks. In a second stage, we describe the only reactive algorithm (WCA). We focus our interest on clustering algorithms dealing with management tasks.

2.1 Proactive Clustering Algorithms

[3] and [4] describe two clustering algorithms aiming to minimize routing information and ensure efficient medium access control. In the first algorithm, called highest connectivity (CON), a node is elected as a clusterhead if it has the highest total number of one hop uncovered neighbors. Any tie is broken by the unique node identification. In the second algorithm, called lowest identification (Lowest-ID), generated clusterheads have the lowest identifications compared to their neighbors. In these two algorithms, the election of clusterheads doesn't take into consideration the quantity of energy existing in the node. Clusterheads are supposed to take in charge many energy consuming functions (routing, security, transmission management…etc) in their clusters. Unlike CON, we can note that Lowest-ID can be improved if identification will be related to energy and mobility.

A variant of CON called K-connectivity identification is described in [6] and [7] where the connectivity degree is computed on k hop neighbors. It generates clusters with k hop members.

In [8], Nocetti, Gonzalez and Stojmenovic describe a K hop clustering algorithm called Max-Min aiming to maximize routes for fault tolerant applications. This algorithm elects clusterheads after two flooding steps called Floodmin and Floodmax. In the first flooding step, every node broadcasts k times (TTL=1) the highest node identification received. In the second step, every node broadcasts k times the lowest node identification received. Then, a node is elected clusterhead if it receives its ID during Floodmin otherwise it elects the minimum node ID received during the two phases as its clusterhead or it elects the maximum node ID received during the first phase as its clusterhead. Experiments show that compared to previously cited algorithm, Max-Min tends to reelect clusterheads after mobility. In addition it generates large clusters with long lifetime clusterheads. This might be an inconvenient since it drops clusterheads battery power because each one will serve a large number of nodes. In addition the election of clusterheads doesn't take into consideration the quantity of energy existing in a node. Moreover, this algorithm generates a very important overhead since it is based on 2*K flooding steps.

In [9], Basagni describes a one hop clustering algorithm called DMAC (Distributed Mobility Adaptative Clustering). Nodes are elected as clusterheads based on a weight calculated on mobility and other parameters which were not specified. This algorithm is better than Lowest-ID and CON because it updates rarely its clusters structure. This might be of a great importance since updating clusterhead frequently results not only in a communication overhead to establish new clusters but also in management information updates.

2.2 Reactive Clustering Algorithms

Here we describe only one reactive clustering algorithm called WCA [5] (Weighted clustering algorithm). In this algorithm, each node broadcasts its weight to all nodes in the network. A node is elected as a clusterhead if it has the Lowest Weight among all uncovered nodes of the network. This process is repeated until all nodes know their roles (a clusterhead or a member). The weight used is a linear function of the node mobility, its connectivity, its consumed energy and the cumulative distance to its neighbors. An elected clusterhead serves a maximum of δ nodes. This helps it saving battery power. Moreover, the algorithm aims to build up efficient transmission management by using low power for intracluster communications and high power for intercluster communications. This minimizes energy consumption and interferences. For the update policy, the clusterhead chooses new clusterheads for its member nodes going far from it. When a node can no longer be a neighbor of any existing clusterhead, it invokes the algorithm to form new clusters. This might be very severe, especially for high mobility and it generates an important computational overhead. Moreover, information stored in the clusterheads (security, administration, policies…etc) should be reestablished after the update phase.

3 The Proposed Clustering Algorithm

We propose a new reactive clustering algorithm, called Lowest Weight (LW) that tries to establish efficient and stable clusters by settling down a convenient metric like

the one specified in WCA [5] while the algorithm layout resembles Lowest-ID [3,4]. The first algorithm specifies a good metric but it generates a high computational overhead. The second algorithm minimizes the number of clustering messages exchanged to settle down clusterheads but uses a bad metric. The proposed algorithm combines the strengths of these two algorithms and specifies a new local update algorithm which minimizes the communication overhead and the nodes reconfigurations after mobility (routing tables and management information such as addressing and security). In what follows, we describe the Lowest Weight clustering algorithm. We give its basis, metric components and its design.

3.1 Basis of Our Clustering Algorithm

The problem of clustering can be seen as follows: given a set of nodes, how can we divide it into an optimal number of clusters without degrading the whole network performances [10]. LW aims to minimize the number of messages exchanged for both clustering and update policy to obtain a lower computational overhead. In case of mobility, it conserves a certain stability of the clusters structure. This is important to avoid re-invoking the algorithm on the whole network and losing the management information stored in the clusterheads.

3.2 The Metric Components

Before computing a metric, we should ask ourselves "clustering for what purpose" and "how can we minimize the generated overhead". In our solution, we aim to better manage the network. This includes all kinds of management (security, administration, transmission management, routing…etc). We can suppose that clusterheads will collaboratively ensure management tasks. To decide how much a node suited for being a clusterhead, we take into consideration the following features, inspired from the WCA metric components:

The Battery Power (BP): Compared to ordinary nodes, clusterheads ensure some services. Thus, we should elect nodes with highest remaining battery power as clusterheads. In WCA, this metric component is computed as the cumulative time Pv, during which a node v acts as a clusterhead. Pv implies how much battery power has been consumed. We have opted to consider the remaining battery power because, in ad hoc networks, at the network bootstrapping, nodes can have different quantities of energy.

The mobility (M): We aim to have stable clusterheads. So we should elect nodes with low mobility as clusterheads. Unlike WCA which computes M from the network bootstrapping till current time T, we compute it as the average speed for the last period of time P, from T-P till current time T as show in equation (1):

$$M = \frac{1}{p} \sum_{t=T-P}^{T} \sqrt{(X_t - X_{t'})^2 + (Y_t - Y_{t'})^2} \quad (1)$$

Where $(X_t - X_{t'})$ *and* $(Y_t - Y_{t'})$ are the coordinates of the node at time t and t'.

We preferred this way to compute M because a node can switch from high (respectively lower) mobility to very lower (respectively very high) one. The node coordinates can be estimated as described in [11].

The Node Connectivity Degree (C): we shouldn't elect nodes with highest connectivity or lowest one as clusterheads. In fact, in the first case, they will be congested and their battery power will drop rapidly. In the second case, the clusters size will be very low and we won't take advantage of clustering. Hello messages are used to compute C. In fact, each node broadcasts a hello message with TTL=1 (including its identification) then uses received hello messages to compute its connectivity degree C.

The Distance to Neighbours (D): it's better to elect a clusterhead with the nearest members. This might minimize node detachments. For a node v, D is computed as the cumulative mean square distance to neighbors divided by the total number of neighbors as shown in equation (2):

$$D = \frac{1}{C} \sum_{v' \in N(v)} \sqrt{(X_v - X_{v'})^2 + (Y_v - Y_{v'})^2} \tag{2}$$

where $(X_v\ Y_v)$ *and* $(X_{v'}\ Y_{v'})$ are the coordinates of the node v and v' respectively and N(v) is v's list of neighbors. These coordinates can be estimated as described in [11]. We assume that this method for computing D is more efficient than the one used in WCA where D is just the cumulative distance to neighbors. In fact, a node with a high number of neighbors close to it can have a distance superior than the one of a node with very few neighbors which are far from it.

3.3 The Proposed Algorithm

LW combines each of the above parameters with certain weighing factors chosen according to the application needs and various networks environment (battlefield, conferencing, vehicular applications…etc). The algorithm is executed for only one time (at the system bootstrapping). Then the updating procedure is locally invoked after mobility or to attach new nodes joining the network. First, we describe clusterheads election procedure. Then, we present the update policy.

Clusterhead Election:
Messages and notations used in the algorithm are described in table 1. Each node:

- Broadcasts a hello message with TTL=1 (including its identification).
- Uses received hello messages to compute its connectivity degree C (total number of neighbors) then computes its weight as shown in equation (3).

$$\begin{aligned} W &= w_1 \times BP + w_2 \times M + w_3 \times C + w_4 \times D \\ where\quad & w_1 + w_2 + w_3 + w_4 = 1 \end{aligned} \tag{3}$$

- Broadcasts its weight to its one hop neighbors (TTL=1)
- Computes a list called neighbor list (NL) that contains the identifications of neighbor nodes and their corresponding weights NL.

If the node possesses the minimum weight compared to the weights in NL it proclaimed itself clusterhead by sending a role message UPDATE_ROLE (My_ID, My_ID) to its one hop neighbors.

If it isn't the case, it expects role messages from its neighbors with lower weights than its one. If it receives at least one role message as clusterhead, it chooses the Lowest Weight node among them. It broadcasts a role message UPDATE_ROLE (My_ID, My_CH_ID) to confirm its role as an ordinary node and attach itself to that clusterhead, identified by My_CH_ID. Otherwise, it becomes a clusterhead and broadcasts a role message UPDATE_ROLE (My_ID, My_ID) to its one hop neighbors.

Table 1. Messages exchanged and notations

Message/notation	Meaning
My_ID	The identification of the node that sends the message
My_CH_ID	The clusterhead identification of the node that sends the message (My ClusterHead IDentification).
UPDATE_ROLE (My_ID, My_CH_ID)	A node sends an update message to declare its role as an ordinary node and attach itself to the clusterhead identified by My_CH_ID.
UPDATE_ROLE (My_ID, My_ID)	A node sends an update message to declare its role as a clusterhead.

Update Policy

The update policy process begins after the election procedure. In our algorithm, we suppose that clusterheads broadcast periodically hello messages. In what follows, we describe how our approach reacts to topology changes.

When an ordinary node moves: When an ordinary node moves within its corresponding cluster (that means that it can join its clusterhead), no changes occurs. Otherwise, the moving node can leave its cluster. Thus, it can find itself closer to multiple or none clusterheads (declared in its neighboring list). In the first case, it chooses the Lowest Weight clusterhead as its new clusterhead and broadcasts its new role as UPDATE_ROLE (My_ID, My_CH_ID). For the second case, the node executes locally the clustering algorithm by sending a hello message to its uncovered neighbours.

When a clusterhead moves: When a clusterhead moves, it leaves its role as a clusterhead until it detects one or numerous clusterheads in its neighborhood. If it has the Lowest Weight, it keeps its role as it is; otherwise it becomes an ordinary node and attaches itself to the Lowest Weight clusterhead by broadcasting an update message UPDATE_ROLE (My_ID, My_CH_ID).

An Illustrative Example

We explain our clustering algorithm execution by applying it on the set of nodes described in Fig 1. Nodes are represented by circles dotted with their identifications. An edge between two nodes exists if each one is on the sight of the other. All existing edges are associated with the corresponding distance between the corresponding two nodes. Table 2 shows, for each node, its metric components as well as the corresponding weight. The two metrics BP and M are arbitrary chosen. The weight factors considered are w1=0.2, w2=0.3, w3=0.2 and w4=0.3.

Table 2. Weight computations for each node

Node ID	C	D	BP	M	Weight
1	4	2.5	2.1	2.33	2.436
2	5	3.4	2.9	1.25	2.85
3	2	2.5	3.6	5.14	2.898
4	2	4	5.5	2.23	3.146
5	2	1	6.3	4.8	2.92
6	4	2.5	2.1	1.78	2.32
7	2	2.5	3.14	5.58	2.894
8	4	1.75	5.21	3.28	3.023
9	2	4	7.12	5.23	4.07
10	3	2	8.4	2.75	3.43
11	4	2.5	2.7	2.14	2.518

Fig 2 shows the clusters identified. In fact, the nodes 1, 6 and 11 declare themselves as clusterheads because each one has the minimum weight compared to the weights of its one hop neighbors. Node 2 chooses 6 as its clusterhead from the set {6, 1 and 11} because 6 have the Lowest Weight...etc.

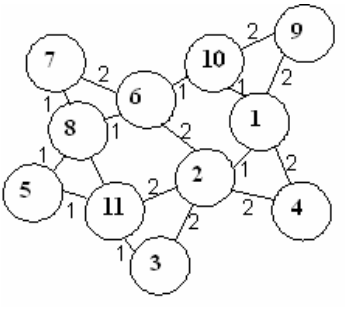


Fig. 1. Nodes with corresponding neighbors and distances

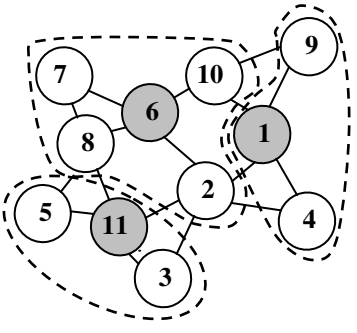


Fig. 2. Clusters identified

4 Main Contributions

Unlike the clustering algorithms described above [3, 4, 6-8], our solution uses a suitable metric since it takes into account the quantity of energy existing in the node and its mobility. Thus, it generates more stable and durable clusterheads. In addition, unlike those solutions, our approach is reactive and it specifies a local update phase while those solutions are proactive. A proactive algorithm is re-invoked periodically even if there's no change in the network topology. This can result in useless exchanged clustering messages and can then degrade the performances of the system.

In comparison with WCA, our approach generates a lower overhead. In fact, each node has to broadcast (TTL=1) only 3 messages to know its role(a hello message for neighbors discovery, a weight message and a role message to declare its role). In WCA [5], each node has to broadcast in the whole network $o(n^2)$ messages to know its role (n is the number of nodes in the network). Moreover, during the algorithm computation, the non covered nodes must re-compute their weights and re-diffuse them. This can lead to a high computational overhead. Furthermore, to decide its role, a node must compare its weight to all weights in the network. But, how does a node know that it received all weights? Thus, WCA might not converge.

We can say also that our approach uses a more adequate update policy. In fact, unlike WCA, we update locally the clusters structure. Moreover, the clustering algorithm is just applied during the network bootstrapping. Then the update phase is executed by each node if it detects special changes in its neighborhood. In WCA, the update phase consists in reapplying the clustering algorithm when a node, can't be attached to any clusterhead. This might change all clusters structure. In fact, all management policies (configurations, security, etc) could be lost and nodes will be obliged to re-establish them.

5 Simulation Experiments

To study our proposed solution and compare its performances to other clustering algorithms, we have extended the NS2 simulator so that it permits to support clustering techniques. Five algorithms were implemented: Lowest-ID, CON, CON-ID, WCA and LW. We focused our study on our proposed algorithm and compare its results essentially to WCA that presents better performances than Lowest-ID.

We fixed three main performance criteria which are:

- clusterheads lifetime
- node reaffiliations
- average number of clusters

These parameters are studied by varying nodes number transmission range and maximum node speed.

The scenarios were generated using the random waypoint model with input parameters such as maximum speed, pause times, number of nodes, area and simulation period. The simulation parameters are listed in Table 3. The weight values used for simulation are w1 = 0.7, w2 = 0.2, w3 = 0.05 and w4 = 0.05.

Table 3. Simulation Parameters

Parameter	Meaning	Value
N	Number of nodes	20 – 60
Grid (m x n)	Scenario area	100 x 100 m^2
Tx	Transmission range	10 – 70m 10 – 120m
PauseT	Pause time	0 sec
MaxSpeed	Maximum speed of nodes	1 – 10 m/s

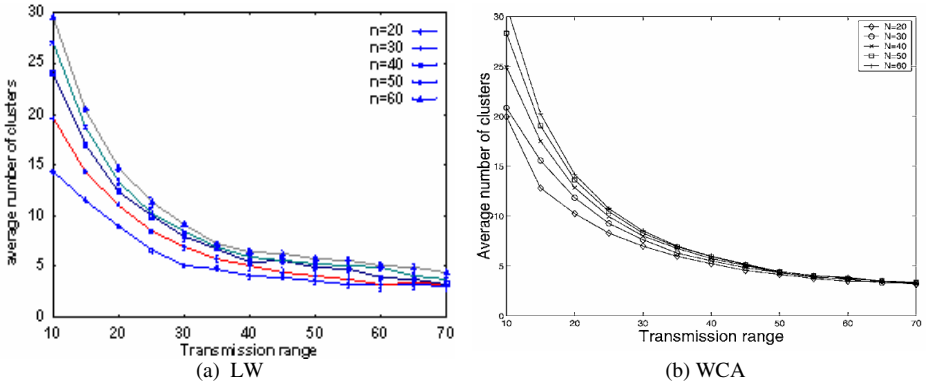
5.1 Discussion of Results

We will discuss results while varying transmission range in a first step and mobility in a second step.

Results for Varying Transmission Range (Tx)

Fig 3 shows, for varying nodes number, the variation of the average number of clusterheads with respect to the transmission range for both LW (a) and WCA (b). The maximum speed was fixed to 5m/s. We notice that the average number of clusterheads decreases with the increase in the transmission range. In fact, a clusterhead with a large transmission range will cover a larger number of nodes.

[12] has shown that an optimum decomposition of a network of n nodes into clusters should be $\sqrt{n}$ clusters of $\sqrt{n}$ members each one. We notice that both LW and WCA give a good clustering of the network. However, for the same simulation parameters, our results are close to that optimum ($\sqrt{n}$). For example, for n=60 and Tx=40, WCA generates 6 clusters while LW generates 7.5 clusters (the optimum for n=60 is 7.74)

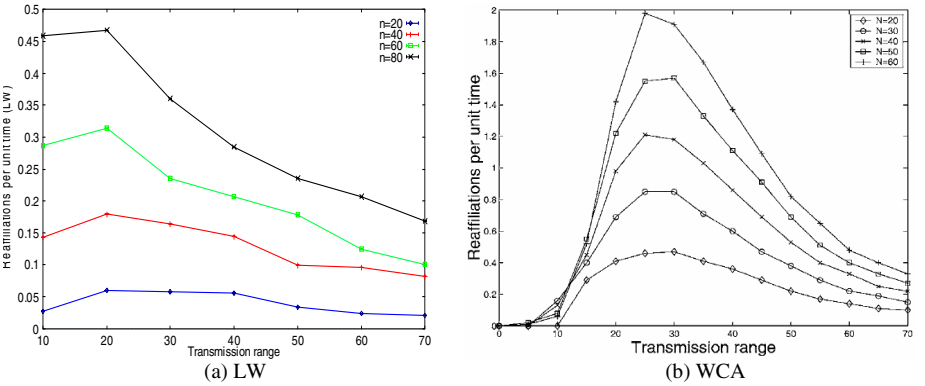


(a) LW (b) WCA

Fig. 3. LW and WCA average number of clusterheads, max_speed = 5

Fig 4 shows the reaffiliations per unit time with respect to the transmission range, where maximum speed is 5m/s. We notice that reaffiliations increases with the increase of transmission range, reaches a peak where transmission range is around 65m, then decreases. This behavior could be explained as follows: for lower transmission range, there are many clusters and the nodes are closer to their clusterheads. Then, while the transmission range increases, clusterheads cover much more moving nodes which can leave the corresponding clusters. After the peak, a clusterhead still cover a large number of nodes which, in spite of their movement, stay in the large area covered by the clusterhead.

In comparison with WCA results, we observe that Lowest Weight results in more stable clusters as it yields as much as 75% reduction in the rate of reaffiliations per unit time. This reduction shows that LW uses a more efficient metric and update procedure than WCA.



(a) LW (b) WCA

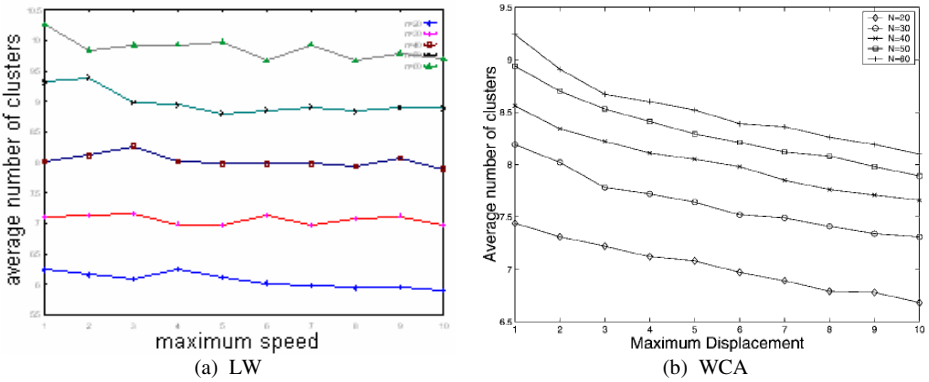
Fig. 4. LW and WCA average number of reaffiliations per unit time, max_speed = 5

Fig 5 shows, clusterheads lifetime with respect to the transmission range where maximum speed is 5m/s. We observe that clusterheads lifetime increases with the increase in the transmission range. This is because, for nodes with higher transmission range, the number of clusterhead decreases and the elected clusterheads are far from each other. Thus, the probability that a moving clusterhead becomes a neighbor of another one is minimized.

Results for Varying Mobility

Fig 5 and 6 show the variation of the same metrics but for varying the nodes maximum speed from 1m/s to 10m/s. In these scenarios, the transmission range is fixed to 30m like in WCA simulations.

Fig 5 (a) shows that, for LW, the average number of clusterheads is almost the same with respect to the maximum speed of nodes. In WCA (Fig 5 (b)), we observe that the number of clusterheads decreases slightly with respect to maximum speed.

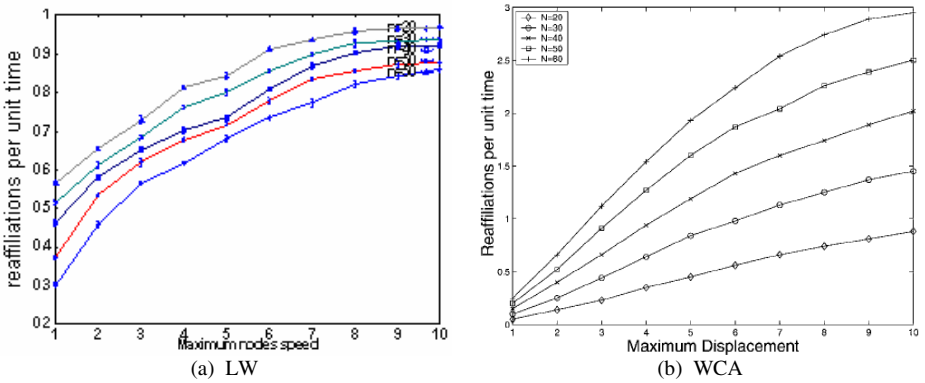


(a) LW (b) WCA

Fig. 5. LW and WCA average number of clusters, Tx=30m

Fig 6 shows the reaffiliations per unit time with respect to the maximum nodes speed where. We notice that reaffiliations increase with the increase of nodes speed. This is because nodes with higher speed quit rapidly their cluster to reach another one.

In comparison with WCA, we observe that our algorithm results in more stable clusters as it yields as much as 60% reduction in the rate of reaffiliations per unit time. In addition, [5] shows that WCA presents the minimum reaffiliation rate compared to Lowest-ID [3, 4], CON [3, 4], CON-ID [6, 8], DCA and DMAC [9]. Compared to WCA results (Fig 6 (b)), we observe that LW generates more stable clusters.



(a) LW (b) WCA

Fig. 6. Reaffiliations per unit time, Tx=30m

6 Conclusions

In this paper, we have proposed a reactive clustering algorithm for ad-hoc networks called Lowest Weight. This algorithm is inspired from two existing algorithms lowest-ID and WCA avoiding their limits. In LW, we have exploited the good strategy of Lowest-ID for clustering. This strategy takes into account only neighbors of a given node while WCA considers the entire network which leads to a great number of clustering messages exchanged between nodes. In selecting clusterheads, we have opted for a metric inspired from the WCA one (the node's degree, mobility, remaining energy and cumulative distance to neighbors). However, we have defined an update procedure that is proper to LW.

We have conducted simulations to evaluate the performances of the LW and compared results essentially to WCA that presents better performances than Lowest-ID. Experiments have shown that LW gives a better clustering than WCA as the number of generated clusterheads is close to the optimum $\sqrt{n}$. In addition, LW results in more stable clusters. Indeed, it allows 30% reduction in the reaffiliation rate per unit time while varying transmission range and 60% while varying mobility.

Our future works will be focused on testing a distributed Public Key Infrastructure over an ad-hoc network structured by the Lowest Weight algorithm.

References

1. S.Sivavkeesar, G.Pavlou, A.Liotta, « Effective management through Prediction base clusering approach in the next generation adhoc networks »
2. M.E.Elhdhili, L.BenAzzouz, F.Kamoun, 2004 “ A Totally Distributed Cluster Based Key Management Model for Ad hoc Networks”. Proc. Med-Hoc-Net 3, pp. 291-299.
3. M. Gerla and J.T.-C. Tsai, 1995,"Multicluster, mobile, multimedia radio network", ACM/Baltzer Journal of Wireless Networks. vol. 1, (no. 3), pp.255-265.
4. C.R. Lin and M. Gerla. 1997, "Adaptive clustering for mobile wireless networks". IEEE Journal on Selected Areas in Communications, Vol. 15, No. 7, pp. 1265-1275.
5. M. Chatterjee, S. K. Das, and D. Turgut, 2002, "WCA : A weighted clustering algorithm for mobile ad hoc networks", ClusterComputing 5, pp. 193-204.
6. G. Chen, F. G. Nocetti, J. S. Gonzalez, and I. Stojmenovic. 2002, "Connectivity Based k-hop Clustering in Wireless Networks". In 35th Hawaii International Conference on System Sciences.
7. A. D. Amis, R. Prakash, T. H.P. Vuong and D. T. Huynh, 2000, "Maxmin Dcluster formation in wireless ad hoc networks," Proc. IEEE Infocom pp. 32-41.
8. F. G. Nocetti, J. S. Gonzalez, and I. Stojmenovic, 2003, "Connectivity Based k-hop Clustering in Wireless Networks." Telecommunication Systems 22, pp. 205-220.
9. S. Basagni, 1999, "Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks". Proceedings of the IEEE Vehicular Technology Conference (VTC), Amsterdam, The Netherlands, pp. 19-22.
10. Charles E. Perkins, ad hoc networking, Addison-Wesley Pub Co, 1st edition December 29, 2000.
11. C. Bettstetter, Giovanni Resta and Paolo Santi, 1993,"The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks," IEEE Trans. Mobile Computing, vol.2, no.3, pp.257-269.
12. L. Kleinrock and F. Kamoun, Hierarchical routing for large networks Performance evaluation and optimization, Computer networks, pp155-174, 11177

Distributed Self-policing Architecture for Fostering Node Cooperation in Wireless Mesh Networks

Lakshmi Santhanam, Nagesh Nandiraju, Younghwan Yoo, and Dharma P. Agrawal

OBR Center for Distributed and Mobile Computing, Department of ECECS
University of Cincinnati, Cincinnati, OH 45221-0030
{santhal, nandirns, ymomo, dpa}@ececs.uc.edu

Abstract. Wireless Mesh Networks (WMNs) are evolving to be the key technology of the future. The self-configuring nature of WMNs and the ease, with which a mesh router/mesh point can be added, makes it pertinent to ensure their secure operation. All the routing protocols in WMNs naively assume the nodes to be co-operative in forwarding each other's packets. However, a node can behave selfishly by discretely dropping other's packets, in an attempt to maximize its throughput. In this paper, we present a distributed scheme called, Distributed Self-policing Architecture for Fostering Node Cooperation (D-SAFNC), for enforcing cooperation among the nodes in a WMN. We use a distributed approach in isolating any selfish node with the help of localized detection agents called sink nodes. We study the effectiveness of our scheme through simulations using ns-2 which reaffirm that D-SAFNC can successfully prevent any performance degradation due to the presence of selfish nodes.

Keywords: Free riders, Mesh networks, Node Misbehavior, Selfish Nodes.

1 Introduction

Recent years have witnessed a rapid evolution of Wireless Mesh Network (WMNs), as seen by the surge in its popularity surpassing well known peer technologies. Since its inception, it has become the limelight of all researchers. Nokia's Rooftop Mesh [1], MIT's roofnet [4], Radiant Networks [3] are some known efforts in this direction.

A WMN excels in performance by providing seamless broadband connectivity [12], when compared to other peer technologies such as cellular and WLAN. A cellular network offers wide area coverage, but provides low channel capacity (at best 3Mbps in 3-G and at best 100 Mbps in 4-G); while the WLANs 802.11 network has an attractive high bandwidth connectivity (802.11g currently in user at 54 Mbps and 802.11n with a theoretical throughput of 540Mbps) but with a very limited range.

A WMN is formed by a set of Access Points (a.k.a mesh routers) connected wirelessly, among which a small subset called the Internet Gateway (IGW), is directly connected to the internet. These mesh routers cooperatively forward each other's packets with an underlying ideology of "using" and "providing" service. This kind of cooperative behavior helps in extending the network coverage without any additional infrastructure. The salient characteristics of WMN include: *scalability, self-healing, and self-configurable capability*.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 147 – 158, 2006.

Although, the notion of ad hoc networking facilitates the plug-and-play architecture there by increasing flexibility, it also increases the vulnerability of the network. A selfish or malicious user can add a rogue Mesh Router (MR) to the network and can start disrupting the network services. Such intermediate router can behave selfishly, by discreetly dropping other's packets and forwarding only its own traffic. A selfish node might not forward another node's traffic with an objective to maximize its throughput. We also call such a node "*free-rider*", as it enjoys network resources without contributing to the community. It is even more precarious if a selfish node is located near the IGW as these nearby nodes are mainly in-charge of forwarding the bulk of traffic in a WMN. This would inordinately affect the multihop flows traversing from distant sources and result in wastage of network resources and cause total havoc to the system.

In order to maintain the system integrity, it is evident all the nodes should cooperatively forward each other's traffic. Authenticating a node is not a complete solution as an intruder could still capture a legitimate node or a legitimate node could later on turn selfish. Hence, we propose a novel distributed self policing architecture to detect such selfishly behaving mesh routers in a WMN. We employ special agents called *sink nodes* that are delegated the duty of policing their local neighborhood to detect free-riders. On identifying *free-rider(s)*, *sink nodes* trigger a system wide alert, instructing rest of the nodes to take preventive measures by quarantining the defaulting nodes. It is quite possible that a free-rider might attempt to accuse an innocent node. Our system can elegantly detect such false accusations by observing the system behavior over a period of time and using an additive increase-multiplicative decrease scheme to relieve the innocent node. Simulation results show that D-SAFNC effectively discourages selfishness by taking timely action against free-riders and fosters cooperation.

The remainder of this paper is organized as follows. We discuss the related work on detecting selfish nodes in multihop ad hoc networks in Section 2, followed by an outline of the assumptions, design goals and challenges in Section 3. We then describe the implementation of the proposed D-SAFNC scheme in Section 4 and present an analysis of its complexity in Section 5. Section 6 discusses the performance evaluation of our scheme. We finally conclude with a summary of the work in Section 7.

2 Related Work

Discouraging selfishness in MANETs (Mobile Ad Hoc Networks) has been widely studied. They adopt either credit-based or reputation-based or game theory based approaches. But, these schemes cannot be directly adopted for WMNs due to several differences in their design. First, WMNs are capable of employing multi-radio multi-channel for simultaneous transmission and reception as a result of which promiscuous listening based reputation scheme cannot be applied. Second, WMNs are relatively static unlike MANETs and hence a credit based scheme fail. Third, the traffic in a WMN is oriented either to or away from the IGW.

In a credit-based scheme (like Nuglets [6], Sprite [16], and PIFA [15]), each node earns virtual currency by forwarding others packets so that they can originate their own packet. They require a tamper-resistant hardware for the authenticity of the

currency or depend on a centralized credit agency to allocate wealth. A central authority is vulnerable to single point of failure as it is overloaded with report messages from all the nodes in the network.

In a reputation based approach, each node promiscuously eavesdrops on the neighboring node's transmission and assigns ratings to each other. The rating is then incorporated by other nodes during their route selection process. Watch-dog and Path-rater model [11] find the selfish nodes by a reputation mechanism. However, it does not take any action against the traffic of a selfish node. Such a neighborhood watch scheme is also prone to a replay attack. CONFIDANT [5] [14] uses a path manager that ranks the paths based on the intermediate nodes along the path, eschewing the selfish node. As the reputation spreads by global flooding, it faces scalability issues. Both schemes, fail to differentiate collision and misbehavior. Game theory approaches fix the forwarding rate of a node at certain Nash equilibrium for the network as in Generous Tit-for-Tat (GTFT) [14], but are realistically infeasible.

CATCH [9] is a distributed scheme for multi-hop wireless network that combines anonymity and Watch-dog approach in detecting free-riders. All nodes broadcast an anonymous message. As the selfish node is unaware of the sender's identity, it is forced to forward all of them dutifully to stay connected. If not, it would risk being isolated from the network. However, this scheme is inapplicable for a WMN employing multi-radio communication, as promiscuous eavesdropping would not be always possible. It also requires each node to possess large memory to store the unsent packets when a neighbor does not forward them. In contrast to all the above schemes, our proposed scheme entails lesser memory overhead due to 2-hop information sharing.

3 Assumptions, Design Goals and Challenges

In this section, we first outline our assumptions, enlist the envisioned goals of D-SAFNC and finally discuss the challenges involved in realizing our goals.

3.1 Assumptions

- We assume that a scheme like ingress filtering can be used to prevent source address spoofing.
- We host sink agents on certain trustworthy mesh routers such that each every node is within the 2-hop neighborhood of a sink agent.
- We assume there is no collusion among selfish nodes. A selfish node is different from a malicious node. A malicious node disrupts the network activity by collusion. In contrast, a selfish node does not gain anything by disrupting the network (in fact by doing so it will defeat its purpose). Its greedy intention to devour all the network resources for itself results in its solitary operation. Hence, this is a safe assumption.

3.2 Design Goals and Challenges

The main design goal of our scheme is to accurately identify selfish nodes and give them a second chance to re-socialize in the network. We target to give each node a

fair chance to originate and immediately transmit packet, irrespective of its geographic location. We stay clear of using a credit or reputation based scheme because of the following inherent flaws [8] [10]:

1. In a credit based scheme, a node positioned in the periphery of the network is handicapped and fails to earn credits as it is not used as an intermediate hop by other nodes. This is very much likely in a WMN wherein nodes located near the IGW forward more data than those at the periphery.
2. As the nodes are not allowed to send traffic until they earn enough credits, it is unsuitable for real-time voice and video applications like VoIP, video conferencing, and video surveillance. When the nodes have insufficient credit, they have to either buffer or drop the unsent traffic, until they earn sufficient credits. This causes undue latency in the packet delivery.
3. In a credit scheme, an egregious node might begin its selfish activity after accumulating enough credits which is counter-intuitive to the goal of the scheme.
4. Most of the credit/reputation schemes are applicable only to a source routing protocol as it needs to determine the credits to be loaded in the packet for transmission.
5. All reputation based schemes require a way to build a reliable mutual trust index by monitoring the network activity. This is in general accomplished by listening to neighboring node's transmissions. However this assumption does not hold well in asymmetrical link [7], and systems with directional antennae [13] or a WMN using multi-radio multi-channel capable nodes (if non-interfering channels are assigned to adjacent nodes).

The aforementioned disadvantages render these approaches impractical for promoting cooperation in WMNs. Thus, we focus on developing a distributed monitoring scheme. As there is a possibility to misclassify a genuine packet loss as misbehavior, it is important to monitor the node behavior over a significant period of time. Moreover the scheme should be resilient to member report losses.

4 Proposed D-SAFNC Scheme

From the discussions in the previous section, we realize that a pervasive solution is essential for monitoring WMN. We start with an overview of the system environment and architecture of D-SAFNC scheme and then proceed to the details of the scheme.

4.1 System Environment and System Architecture

We consider a static framework of interconnected nodes forming a mesh topology that provides wireless internet service in an office or a university as shown in Fig. 1. In order to facilitate simultaneous communication with the end users and other mesh routers, we assume that each mesh router has at least two interfaces operating on non-interfering channels.

We propose a distributed scheme, D-SAFNC; which helps in detecting free-riders by deploying sink agents at about 10% of the routers in the network. System

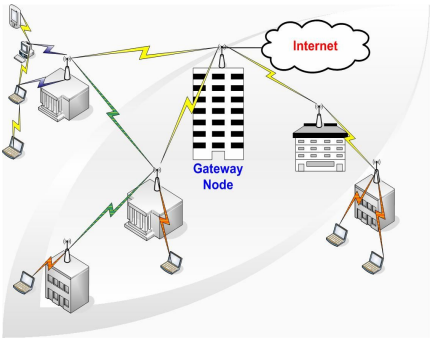


Fig. 1. A WMN in a University

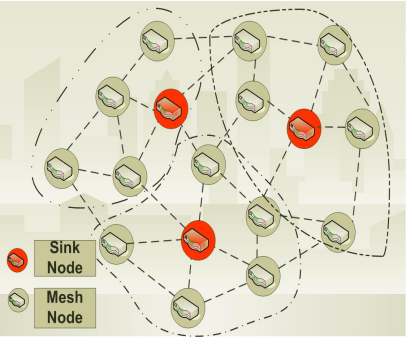


Fig. 2. Monitoring using Sink Nodes

monitoring is divided into two phases: Start-up phase and Monitoring phase. In the *start-up phase*, the sink agents as shown in Fig. 2 advertise their presence by sending periodic beacons. Each mesh router upon receiving a beacon registers itself under the sink in two cases:

- If it has not already selected any sink or
- If the new sink is nearer than the previously registered sink.

To regulate the flooding of beacons each mesh node rebroadcasts the beacon only if the hop-count is less than BEACON_MAX_HOPS. In the *monitoring phase,* once all the mesh routers are aware of their respective sinks, they send periodic reports to the sinks every REPORT_ROUND time. Unlike SPRITE [16] that sends a report for every forwarding message, this aggregated scheme saves considerable overhead in terms of network bandwidth and payload. The periodic report consists of information on the number of packets received and forwarded by a node during a certain interval of time. Table 1 gives a brief definition of each field in the report message.

At end of REPORT_ROUND time, each sink applies the following three checkpoints. First, it computes a simple check between the output of a node and the input registered at its neighbor, as given in Equation (1). It checks for every link if the output from a node is same as the input at its neighbor. Let A_j and A_k denote the set of neighbors of node j and k respectively. If j and k are two neighboring nodes, then

$$O_{j,k} = I_{k,j} (j \in A_k, k \in A_j) \tag{1}$$

Where $O_{j,k}$ and $I_{k,j}$ denote the O and I fields of a message report whose IDR and IDN are j and k. This computation prevents any node from dropping packets.

Second, it checks if S, if the number of packets originating at current node j as reported by $node_j$ is equal to NON i.e. number of packets that originated at node j among input packets from node j to node k as reported by $node_k$. This check prevents a node from misreporting the number of packets that are originating from a given node.

$$S_{j,k} = NON_{k,j} (j \in A_k, k \in A_j) \tag{2}$$

The third and final check, finds the number of packets forwarded F_j by a node j using the two formulae and compares them. Equation (3) computes the total number of packets forwarded by a node j to all its neighbors (excluding its own packets). Equation (4) computes the packets forwarded by node j based on its neighboring node's (node k) reports i.e. the difference between total number of input packets to a node j and the total number of packets terminating at node j. Equation (3) and (4) should be equal to ensure that a selfish node does not manipulate the value of S or O.

$$F_j = \sum_{k \in A_j} O_{j,k} - \sum_{k \in A_j} S_{j,k} \tag{3}$$

$$F_j = \sum_{k \in A_j} I_{j,k} - \sum_{k \in A_j} NTC_{j,k} \tag{4}$$

There is a possibility of packet loss occurring due to interferences/channel degradation/queuing overflows in a wireless channel which should not be misinterpreted as selfish behavior. Hence, when the three checkpoints are applied, we always consider maximum permissible packet drop for a given network condition.

Table 1. Format of Report Messages

IDR	ID of the reporting node
IDN	ID of the neighboring node
IDS	ID of the node's registered local sink
SEQ	Sequence number of the node's report for synchronizing member reports at the sink
I	No. of input packets from the neighbor
O	No. of output packets to the neighbor
S	No. of packets originating at current node among the output packets to the neighbor
NON	No. of packets that originated at the neighbor among the input packets from the neighbor
NTN	No. of packets terminated at next hop (at IDN) among the packets sent from IDR to IDN.
NTC	No. of packets terminating at this current node (at IDR)

When a new node joins the network, it first registers itself to its nearest sink node and then places a request to the sink. The sink replies to the new node with the current sequence number being used, reply time and REPORT_ROUND time. The new node computes the new sequence number as given by Equation (5).

$$New\_SEQ = SEQ + [\frac{Current\_time - Reply\_time}{REPORT\_ROUND}] \tag{5}$$

4.2 Free Rider Detection Algorithm

The system runs a *free-rider detection algorithm* at every CHECK_ROUND time (= 4 * REPORT_ROUND time) that accurately identifies and punishes the free-rider. After applying the three checkpoints on its member reports, each sink checks if reports from two adjacent nodes do not accord with each other. If so, the node and the neighbor involved in the transaction is added to a NAM (Number of Alleged Manipulation) list maintained at the sink.

Looking at the inconsistencies at a single sink node, the identity of the free-rider is unclear, as member nodes involved in the alleged manipulations might belong to the same domain (intra) or a different domain (intra). Hence, one sink node is chosen as a sink manager (SM) to which all other sinks nodes unicast their NAM list. A master NAM list is created at the SM. As only the suspicious node list is passed to the SM, D-SAFNC when compared to a completely centralized scheme incurs lesser overhead in evaluating reports and lesser congestion, at each sink.

Using the master NAM list, the SM then builds an Inconsistency Record Table (IRT) as shown in Table 2. Each entry $m_{a,b}$ in IRT represents the number of alleged manipulations in the packet transmission between node *a* and *b*. The last column denotes the total NAM values for each node. If this is greater than a certain threshold (UT_PERMISSIBLE_MANIPULATIONS- *for a node not in blacklisted history*) *and* (LT_PERMISSIBLE_MANIPULATIONS- *for a node in blacklisted history*), this node is blacklisted and added to a blacklisted node history. Each entry $m_{a,b}$ is incremented in the IRT by an additive increase and multiplicative decrease algorithm. This is done so that an innocent node is not unduly framed and punished. For example, if there is an inconsistency between node a's and b's report, we increase the NAM values given by Equation (6).

$$m_{a,b} = m_{a,b} + 1 \text{ and } m_{b,a} = m_{b,a} + 1 \tag{6}$$

As other nodes involved in a transaction with a or b might be penalized, the $m_{i,a}$ and $m_{i,b}$ values of other nodes are reduced by half given by Equation (7).

$$m_{i,a} = \frac{m_{i,a}}{2} \forall\ i \notin \{a, b\} \text{ and } m_{i,b} = \frac{m_{i,b}}{2} \forall\ i \notin \{a, b\} \tag{7}$$

Once a blacklisted node is detected, the SM announces it to the entire network. Upon receiving this message, the nodes that have route through this blacklisted node invalidate their entries and take appropriate re-routing action. In AODV, this can be either performing a local repair or sending a route error to the source (RERR). Thus the affected nodes now reroute their traffic through alternate paths.

Selfish behavior is discouraged as all the legitimate nodes collectively refuse to forward any traffic originating from the blacklisted node. SM maintains the list of all

Table 2. Inconsistency Record Table

	A	B	C	…	Total
A	-	$m_{a,b}$	$m_{a,c}$	…	$\sum m_{a,i}$
B	$m_{b,a}$	-	$m_{b,c}$	…	$\sum m_{b,i}$
C	$m_{c,a}$	$m_{c,b}$	-	…	$\sum m_{c,i}$
…	…	…	…	…	…

previously blacklisted nodes along with the observed time of its misbehavior. A free-rider is not permanently blacklisted; instead its isolation is associated with a timer (FORGIVEN_TIME). On the expiration of this timer, the system temporarily pardons the isolated node to give it a second chance. The other nodes henceforth resume routing through this node. If the node begins its selfish activity at any time in the future and is found in the NAM list, its threshold for IRT table computation is lowered to LT_PERMISSIBLE_MANIPULATIONS as a precautionary measure. Using the IRT computation, if it is found to default again, it is *permanently blacklisted.* Other nodes permanently shun any traffic originating from this node and never consider routing through this blacklisted node. Thus transient liars that oscillate between good and bad behavior are successfully caught and punished.

5 Complexity Analysis

In this section, we analyze the message complexity of the proposed D-SAFNC. There are two kinds of messages: one is the report to the local sink from a WMN nodes and the other is the inconsistency information to the SM from local sinks. However, since the amount of the inconsistency information is just equal to the number of sink agents, this inconsistency information is not a large overhead if we assume optimal minimum number of sinks in a WMN. Thus, the analysis focuses on the member reports submitted periodically every REPORT_ROUND to the local sink agent.

The notations are as follows:
A: total area of a WMN
N: total number of WMN nodes
r: transmission range of each node
s: number of sink agents
c: number of nodes associated with one sink agent
b: number of neighboring nodes of a WMN node

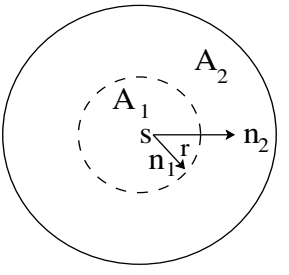


Fig. 3. Coverage of One Sink Node

We note that the number of sink agents, s, is determined so that every WMN node may reach at least one sink within two hops. Assuming all WMN nodes are uniformly distributed, the area a sink can maximally cover is $4\pi r^2$ as shown in Fig. 3. Hence, at least $\left\lceil \frac{A}{4\pi r^2} \right\rceil$ sink agents are needed. Considering minimum number of sink nodes, the number of WMN nodes a sink should manage is $c = \frac{4\pi r^2 N}{A}$. Each WMN node sends reports for every neighbor, and the average number of

neighbors of one given node in a uniformly distributed network is $b = \frac{\pi r^2 N}{A} - 1$.

Hence, each sink agent receives as many reports as cb every REPORT_ROUND, and the total number of reports in a WMN using D-SAFNC is given by following Equation (8):

$$scb \geq \left\lceil \frac{A}{4\pi r^2} \right\rceil \cdot \frac{4\pi r^2 N}{A} \left(\frac{\pi r^2 N}{A} - 1 \right) \tag{8}$$

Meanwhile, the total hop count of report messages can be computed as follows. In Fig. 3, as A_2 is three times wider than A_1, we can safely assume that A_2 includes three times as many nodes as A_1. Since a node in A_1 and A_2 can reach the sink with one hop and two hops respectively, the average hop count, is $h = (1 \times 1 + 2 \times 3)/4 = 1.75$. Thus, the total hop count required for report messages is $1.75scb$.

6 Performance Analysis

In this section, we evaluate the performance of D-SAFNC using ns-2 simulator [1]. Although D-SAFNC can be run on top of any underlying routing protocol, we choose AODV as the routing protocol. We consider a network of 25 mesh points in a 5x5 grid (shown in Fig 4(a)) spread over an area of 1500m x 1500m. IEEE 802.11 is used for channel arbitration with the transmission range and channel capacity set to 250 m and 11 Mbps respectively. The total simulation time is set to 200 seconds. We set D-SAFNC specific parameters as follows: CHECK_ROUND (28 sec), REPORT_ROUND (7 sec), LT_PERMISSIBLE_MANIPULATIONS (1 sec), FORGIVEN_TIME (14 sec), BEACON_MAX_HOPS (2), and UT_PERMISSIBLE_ MANIPULATIONS (3 sec).

6.1 Instantaneous Throughput

To evaluate the effectiveness of our scheme in the presence of selfish nodes, we study the fluctuations in the instantaneous throughput of the flows. We start two flows (Flow 1 and 2) in both directions between mesh routers MR 0 and MR 20 (which is an Internet GW) as shown in Fig. 4(a) at time equal to 1 second. We place a selfish node (MR 10 in Fig. 4(a)) in the shortest path between the two nodes. At time 10 seconds, we start a traffic flow from this misbehaving node to the IGW. As seen from the Fig. 4(b) and 4(c) during the time period 1-30 seconds, both the flows from the good nodes (MR 0 & MR 20) suffer from 100% packet loss as they choose their routes through the selfish node (MR 10).

On the other hand, the flow from MR 10 enjoys good throughput, Fig. 4(e). However this free-riding does not continue for a long period of time. After four rounds (nearly 30 seconds) of continued misbehavior by MR 10, the SM confirms MR 10 as a free-rider and broadcasts this information to the entire network. Thus, MR 5 and MR 15 which have active routes through MR 10 purge their routing entry and

re-route their traffic. This is clearly illustrated from the Fig. 4(b) & (c) during the time period 40-200 seconds. At the same time, neighbors of the selfish node (MR 5 and MR 15) stop forwarding any traffic originating from MR 10 and thus the flows from MR 10 are shut albeit for a short period of time (FORGIVEN_TIME).

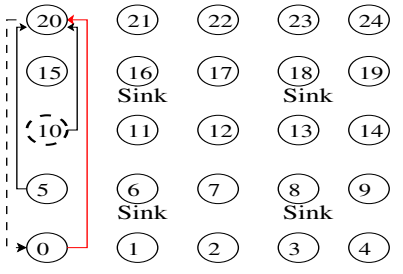


Fig. 4(a). Grid Network

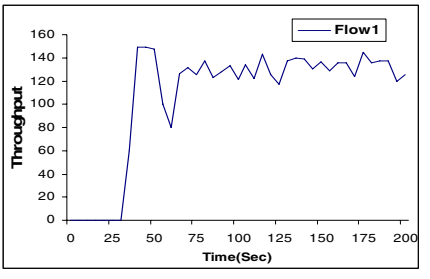


Fig. 4(b). Flow 1 (between 0-20)

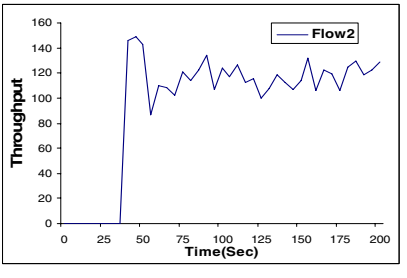


Fig. 4(c). Flow 2 (between 20-0)

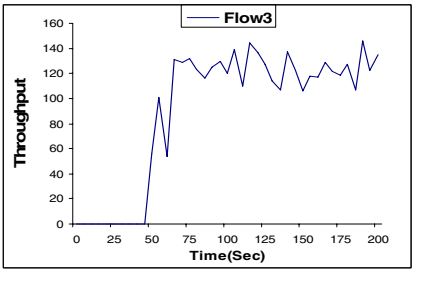


Fig. 4(d). Flow 3 (between 5-20)

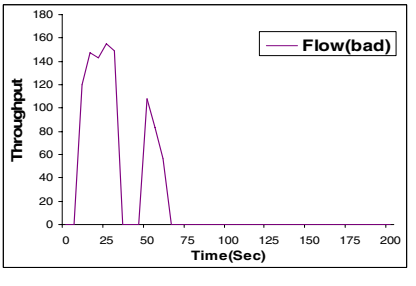


Fig. 4(e). Bad Flow (between 10-20)

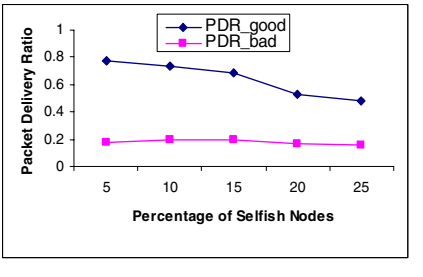


Fig. 5. PDR vs. % of selfish nodes

In order to illustrate the punishment for prolonged misbehavior, we start another flow from MR 5 towards the IGW (Flow 3 in Fig. 4(d)) shortly after the selfish node is forgiven. MR 5 will now consider routing its traffic through MR 10 as it is on its shortest path to MR 20. However as MR 10 continues its misbehavior, flow from MR

5 suffers 100% packet loss. This can be seen during the time period 45-65 seconds in Fig. 4(d). The SM quickly identifies the misbehavior of MR 10, permanently blacklists it and then notifies to the entire network. MR 5 now tries to reroute its traffic through an alternate route. From this point on, MR 10 which is permanently blacklisted will not be able to route any traffic in the network. This can be seen from the Fig. 4(e) during the time period 75-200 seconds.

6.2 Packet Delivery Ratio

We now evaluate the effectiveness of D-SAFNC in the presence of multiple selfish nodes. We measure the Packet Delivery Ratio (PDR), which is the ratio of the number of packets received at the destination to the number of packets generated at the source.

We randomly pick different source MRs and IGWs and start traffic from these nodes. Fig. 5 shows the PDR of the good and bad nodes for varying percentage of selfish nodes. As can be seen from Fig. 5, D-SAFNC ensures that PDR of good nodes is well maintained while considerably throttling the PDR of bad nodes. Even though good nodes may occasionally loose packets because of the presence of selfish nodes in their path, they quickly recover and try to reroute the traffic, consequently maintaining a steady PDR. As D-SAFNC gives a second chance to the misbehaving node, the PDR of free-riders is low but non zero as indicated by the PDR_bad plot in Fig. 5.

PDR of good nodes decreases as we increase percentage of selfish nodes. This is because as we increase the number of selfish nodes we also increase the traffic flows as a result increasing the load on the network. Also, packets from good nodes experience some loss during re-routing process, as now they take longer hops to reach their destination. However, D-SAFNC prevents the PDR of good nodes from dropping below 50% even when 25% of the nodes are selfish.

7 Conclusion

Mesh networks are continuously gathering momentum in its evolution in the wireless industry which also raises several security concerns. We highlighted the inadequacy of credit/reputation based schemes in promoting cooperation in a WMN and presented a distributed policing architecture. As the information sharing of member reports is restricted to a two hop neighborhood, it has considerably less overhead as compared to a centralized scheme. These are fortified by the simulation results which indicate that D-SAFNC increases the throughput of the system. The system tries as much as possible to re-accommodate even the past misbehaving nodes and this way fosters cooperation among the mesh routers. In our future work, we plan to implement the scheme using multi-channel multiple interface architecture such that backhaul links of different frequency are for sending reports to the sink.

Acknowledgement. This work has been partially supported by the Ohio Board of Regents, Doctoral Enhancement Funds.

References

[1] Network Simulator (NS-2), http://www.isi.edu/nsnam/ns/index.html.
[2] Nokia RoofTop Wireless Routing. White paper.
[3] Radiant Networks Website – www.radiantnetworks.co.uk
[4] Aguayo, D., Bicket, J., Biswas, S., Judd, G., Morris, R.: Link-level Measurements from an 802.11b Mesh Network. In: the Proc. of SIGCOMM. (2004)
[5] Buchegger, S., Boudec, J.-Y. L.: Performance analysis of the CONFIDANT protocol: Cooperation of nodes- fairness in dynamic ad-hoc networks. In: the Proc of MobiHOC. (2002)
[6] Buttyan, L., Hubaux, J.-P.: Enforcing Service Availability in Mobile Ad-Hoc WANs. In: the Proc of IEEE/ACM MobiHOC Workshop. (2000)
[7] De Couto, D., Aguayo, D., Bicket, J., Morris, R.: A High-Throughput Path Metric for Multi-Hop Wireless Routing. In: the Proc. of ACM MobiCom. (2003)
[8] Huang, E., Crowcroft, J., Wassell, I.: Rethinking incentives for mobile ad hoc networks. In: the Proc. of ACM SIGCOMM PINS. (2004)
[9] Mahajan, R., Rodrig, M., Wetherall, D., Zahorjan, J.: Sustaining Cooperation in Multi-Hop Wireless Networks. In: the Proc. of NSDI. (2005)
[10] Mahajan, R., Rodrig, M., Wetherall, D., Zahorjan, J.: Experiences Applying Game Theory to System Design. In: the Proc. of ACM SIGCOMM. (2004)
[11] Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating router misbehavior in mobile ad-hoc networks. In: the Proc. of Mobi-Com. (2000)
[12] Poor, R., Corp, E.: Wireless MESH Network. In: Intelligent System – Wireless. (2003)
[13] Saha, A.K., Johnson, D.B.: Routing improvement using directional antennas in mobile ad hoc networks**.** In: the Proc. of IEEE GlobeCom, Vol.5. (2004) 2902 – 2908
[14] Srinivasan, V., Nuggehalli, P., Chiasserini, C.F., Rao, R.R.: Cooperation in wireless ad hoc networks. In: the Proc. of IEEE INFOCOM. (2003)
[15] Yoo, Y., Ahn, S., Agrawal, D.P.: A Credit-Payment Scheme for Packet Forwarding Fairness in Mobile Ad hoc Networks. In: the Proc. of IEEE ICC. (2005)
[16] Zhong, S., Yang, Y., Chen, J.: Sprite: A simple, cheatproof, credit-based system for mobile ad hoc networks. In: the Proc. of IEEE INFOCOM. (2003)

RFID Systems: A Survey on Security Threats and Proposed Solutions

Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda

Computer Science Department, Carlos III University of Madrid
{pperis, jcesar, jestevez, arturo}@inf.uc3m.es

Abstract. Low-cost Radio Frequency Identification (RFID) tags affixed to consumer items as smart labels are emerging as one of the most pervasive computing technology in history. This can have huge security implications. The present article surveys the most important technical security challenges of RFID systems. We first provide a brief summary of the most relevant standards related to this technology. Next, we present an overview about the state of the art on RFID security, addressing both the functional aspects and the security risks and threats associated to its use. Finally, we analyze the main security solutions proposed until date.

Keywords: RFID Security, Pervasive Computing, Ubiquitous Computing, Security and Privacy.

1 Introduction

At the moment, the most extended identification systems are barcodes. Initially, there were two standards: the Universal Product Code (UPC, United States) and the European Article Number (EAN, Europe). Although, at first, EAN was only taken by twelve European countries, by the end of 2004 more than one hundred countries all over the world had already adopted this standard. Finally, when the United States decided to adopt the European-born standard, UPC and EAN merged, giving rise to what is nowadays known as GS1 [8].

Recently, the mass deployment of Radio Frequency Identification systems (RFID) has taken place. These systems comprise of Radio Frequency (RF) tags or transponders, and RF readers or transceivers. Tag readers broadcast an RF signal to access resistant data stored in tags. One of the main differences with barcodes is that RFID tags provide an unique identifier, or a pseudonym that allows accessing to this unique identifier. The use of RFID tags offers several advantages over barcodes: data can be read automatically, without line of sight, and through a non-conducting material such as cardboard or paper, at a rate of hundreds of times per second, and from a distance of several meters.

Radio frequency identification systems are becoming valuable tools in processes such as manufacturing, provision chain management, and stock control. Around 5 billion barcodes are read daily, so efficiency gains from using

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 159–170, 2006.

RFID tags could substantially lower the cost of tagged items [29]. The penetration of RFID systems is nowadays mainly limited by privacy concerns and by their cost, which must be between 0.05 and 0.1 € to be considered affordable. Additionally, in order to take full advantage of the potential offered by RFID tags, the identification of an item must be made throughout all its life cycle: production, distribution, sale and recycling.

The low cost demanded for RFID tags causes them to be very resource limited. Typically, they can only store hundreds of bits, roughly have between 5000 and 10000 logic gates, and a maximum communication range of a few meters. Within this gate counting, only between 250 and 3000 gates can be devoted to security functions. It is interesting to recall that for a standard implementation of the Advanced Encryption Standard (AES) between 20000 and 30000 gates are needed. Additionally, power restrictions should be taken into account, since most RFID tags in use are passive. Furthermore, one can not suppose either that these systems are able to store passwords in a secure way, because tags are not resistant against tampering attacks at all.

In spite of all these limitations, the penetration of RFID technology is increasing steadily. Experts believe that both systems will coexist some time and that finally, RFID tags will completely replace classical barcodes. An example of this increasing interest in RFID technology is the project of the European Central Bank about including RFID tags in 500 € bills, along with barcodes.

Nevertheless, the implantation of RFID systems is not being absolutely spotless, as there are some organizations like CASPIAN [4] which are strongly against their massive deployment.

2 Overview of RFID Systems

2.1 RFID System Components

RFID systems are made up of three main components, that we briefly describe in the following: the transponder or RFID tag, the transceiver or RFID reader, and the back-end database.

1. ***Transponder or RFID Tag***
   In an RFID system, each object will be labeled with a tag. Each tag contains a microchip with some computation and storage capabilities, and a coupling element, such as an antenna coil for communication. Tags can be classified according to two main criteria:
   - The type of memory: read-only, write-once read-many, or fully rewritable.
   - The source of power: active, semi-passive, and passive.
2. ***Transceiver or RFID Reader***
   RFID readers are generally composed of an RF module, a control unit, and a coupling element to interrogate electronic tags via RF communication. Readers may have better internal storage and processing capabilities, and frequently connect to back-end databases. Complex computations, such as all kind of cryptographic operations, may be carried out by RFID readers,

as they usually do not have more limitations than those found in modern handheld devices or PDAs.

3. ***Back-end Database***
   The information provided by tags is usually an index to a back-end database (pointers, randomized IDs, etc.). This limits the information stored in tags to only a few bits, typically 96, which is a sensible choice due to tag severe limitations in processing and storing. It is generally assumed that the connection between readers and back-end databases is secure, because processing and storing constraints are not so tight in readers, and common solutions such as SSL/TLS can be used.

2.2 RFID System Interface

In this section, we focus exclusively on passive RFID tags, since we consider that these will be the first to be massively deployed and form part of our daily lives. Additionally, these low-cost RFID systems are very limited on resources, which forces some interesting trade-offs in their designs.

1. ***Transceiver/Transponder Coupling Communication***
   Passive RFID tags obtain their operating power by harvesting energy from the electromagnetic field of the reader communication signal. Two main possibilities exist here: near field ($d < \frac{1}{2\pi f}$) and far field ($d > \frac{1}{2\pi f}$) [2].

   The signal sent from readers to tags must be used simultaneously to transmit both information and energy. However, readers normally operate in Industrial Scientific-Medical (ISM) bands, so there are restrictions in the bandwidth and in the transmitted power. Tags, on the other hand, are not under these limitations.
2. ***Data Coding***
   The exchange of data between the reader and the tag, and vice versa, must be performed efficiently; so both coding and modulation are used. The coding/modulation is defined according to the existing limitations in the backward and the forward channel. Readers will be able to transmit greater power, but will have bandwidth limitations. Tags, which are passive, will not have bandwidth limitations.

   As a coding mechanism, level codes (Non-Return-to-Zero, NRZ; and Return to Zero, RZ) or transition codes (Pulse Pause Modulation, PPM; Pulse Weight Modulation, PWM; and Manchester) are mostly used. These coding techniques are depicted in *Table* 1.

Table 1. Coding Techniques

Channel	Usual Coding
Forward Channel	Manchester or NRZ
Backward Channel	PPM or PWM

3. ***Modulation***
   The modulation scheme determines how the bitstream is transmitted between readers and tags, and vice versa. Three possible solutions exist: Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK) and Phase Shift Keying (PSK). The choice of a modulation type is based on power consumption, reliability, and bandwidth requirements.
4. ***Tag Anti-collision***
   Collisions in RFID systems happen when multiple tags simultaneously answer to a reader signal. Methods used to solve this kind of problems, allowing reliable communication between readers and tags, are referred to as anti-collision methods. The anti-collision algorithms used in RFID systems are quite similar to those applied in networks, but they take into account that RFID tags are generally more limited than the average network device. Two approaches are used: probabilistic or deterministic. However, in practice, many solutions are a combination of both.
5. ***Reader Anti-collision***
   In this case, several readers interrogate the same tag at the same time. This is known in the bibliography as the *Reader Collision Problem*. One possible solution to this problem consists of allocating frequencies over time to a set of readers by either a distributed or a centralized approach.
6. ***Frequencies and Regulations***
   Most RFID systems operate in ISM bands [15]. ISM Bands are designated by the International Union of Telecommunications and are freely available to be used by low-power, short-range systems. The most commonly used ISM frequencies for RFID systems are 13.56 MHz and 902-928 MHz (only in the US). Each band has its own radiation power and bandwidth regulations.

3 RFID Standards

RFID systems do not lack standards. Those standards typically describe the physical and the link layers, covering aspects such as the air interface, anti-collision mechanisms, communication protocols and security functions. Nevertheless, not everything is well covered, and there is a certain absence of standardization in testing methods and application data (notably in protocols and application programming interfaces).

3.1 Contactless Integrated Circuit Cards

ISO 7810 defines a special type of identification cards without contact. According to the communication range, three types of cards can be distinguished:

- Close-coupled cards (ISO 10536). These are cards that operate at a very short distance of the reader (< 1 centimeter).
- Proximity cards (ISO 14443). These are cards that operate at an approximated distance of 10 centimeters of the reader. They can be considered as a high-end RFID transponder since they have a microprocessor.

– Vicinity cards (ISO 15693). These are cards that operate at distances greater than one meter. On the contrary to the previous cards (ISO 14443), they usually only incorporate inexpensive machines of states, instead of microprocessors.

3.2 RFID in Animals

ISO 11784, ISO 11785, and ISO 14223 standardize tags for animal identification in the frequency band below 135 KHz. Initially, standards define an identifier of 64 bits. In ISO 14223, greater blocks for reading and writing, as well as blocks of protected writing, are allowed. There are hardly any differences between the communication protocols defined in ISO 14223 and ISO 18000-2.

3.3 Item Management

ISO 18000 defines the air interface, collision detection mechanisms, and the communication protocol for item tags in different frequency bands.

– Part 1 describes the reference architecture.
– Parts 2-7 specify the system in different frequency bands (<135KHz, 13.56 MHz, 2.45 GHz, 5.8 GHz, 900 MHz, and 433 MHz).

3.4 Near-Field Communication (NFC)

1. ***NFCIP-1***
   NFC is designed for interactions between tags and electronic devices in close proximity (< 10 cm). The standards ETSI TS 102.190, ISO 18092, and ECMA 340 identically define the Near Field Communications Interface and Protocol-1 (NFCIP-1).

   These protocols describe the air interface, initialization, collision avoidance, a frame format, and a block-oriented data-exchange protocol with error handling. Additionally, they describe two different communication modes: active and passive.
2. ***NFCIP-2***
   The Near Field Communication Interface and Protocol-2 (NFCIP-2) specifies the communication mode selection mechanism (ECMA 352). NFCIP-2 compliant devices can enter in three different communication modes: NFCIP-1, ISO 14443, and ISO 15693. All these modes operate at 13.56 MHz and are designed not to disturb other RF fields at the same frequency.

3.5 Electronic Product Code (EPC)

The Auto-ID (Automatic Identification) Center was created in October 1999 at the MIT Department of Mechanical Engineering, by a number of leading figures. At the beginning, EPC was developed by the Auto-ID Center. The Auto-ID Center officially closed the 26th October, 2003. The center had completed its work and transferred his technology to EPCglobal [9]. EPCglobal is a joint venture between EAN International and the Uniform Code Council (UCC). The so-called EPC network is composed of five functional elements:

- The Electronic Product Code is a 96-bit number with 4 distinct fields: identifying the EPC version number, domains, object classes, and individual instances.
- An Identification System which consists of RFID tags and readers. Tags can be of three different kinds (Class 0, 1, and 2). The Auto-ID Center published a protocol specification for Class 1 tags in the HF band (compatible with ISO 15693 and ISO 18000-3), and Class 0 and 1 tags in the UHF band.
- The Savant Middleware offers processing modules or services to reduce load and network traffic within the back-end systems.
- The Object Naming Service (ONS) is a network service similar to the Domain Name Service (DNS), which is a technology capable of handling the volumes of data expected in an EPC RFID system.

4 Risks and Threats

Although RFID systems may emerge as one of the most pervasive computing technologies in history, there are still a vast number of problems that need to be solved before their massive deployment. One of the fundamental issues still to be addressed is privacy. Products labeled with tags reveal sensitive information when queried by readers, and they do it indiscriminately.

A problem closely related to privacy is tracking, or violations of location privacy. This is possible because the answers provided by tags are usually predictable: in fact, most of the times, tags provide always the same identifier, which will allow a third party to easily establish an association between a given tag and its holder or owner. Even in the case in which tags try not to reveal any kind of valuable information that could be used to identify themselves or their holder, there are many situations where, by using an assembly of tags (constellation), this tracking will still be possible.

Although the two aforementioned problems are the most important security questions that arise from RFID technology, there are some others worth to mention:

1. ***Physical Attacks***
   In order to mount these attacks, it is necessary to manipulate tags physically, generally in a laboratory. Some examples of physical attacks are probe attacks, material removal through shaped charges or water etching, radiation imprinting, circuit disruption, and clock glitching, among others. RFID tags offer little or none resilience against these attacks.
2. ***Denial of Service (DoS)***
   A common example of this type of attack in RFID systems is the signal jamming of RF channels.
3. ***Counterfeiting***
   There are attacks that consist in modifying the identity of an item, generally by means of tag manipulation.
4. ***Spoofing***
   When an attacker is able to successfully impersonate a legitimate tag as, for example, in a man-in-the-middle attack.

5. ***Eavesdropping***
   In this type of attacks, unintended recipients are able to intercept and read messages.
6. ***Traffic analysis***
   Describes the process of intercepting and examining messages in order to extract information from patterns in communication. It can be performed even when the messages are encrypted and can not be decrypted. In general, the greater the number of messages observed, the more information can be inferred from the traffic.

5 Proposed Solutions

In this section we present the best solutions proposed so far to solve the security problems and threats associated with the use of RFID systems. Our objective is not to give a detailed explanation of each solution, but to provide the reader with the fundamental principles and a critical review of every proposal, as well as the bibliography to be checked in case someone wishes to deepen on some aspects of this subject.

5.1 Kill Command

This solution was proposed by the Auto-ID Center [5] and EPCglobal. In this scheme, each tag has a unique password, for example of 24 bits, which is programmed at the time of manufacture. Upon receiving the correct password, the tag will deactivate forever.

5.2 The Faraday Cage Approach

Another way of protecting the privacy of objects labeled with RFID tags is by isolating them from any kind of electromagnetic waves. This can be made using what is known as a Faraday Cage (FC), a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies). There are currently a number of companies that sell this type of solution [24].

5.3 The Active Jamming Approach

Another way of obtaining isolation from electromagnetic waves, and an alternative to the FC approach, is by disturbing the radio channel, a method which is known as active jamming of RF signals. This disturbance may be done with a device that actively broadcasts radio signals, so as to completely disrupt the radio channel, thus preventing the normal operation of RFID readers.

5.4 Blocker Tag

If more than one tag answers a query sent by a reader, it detects a collision. The most important singulation protocols are ALOHA (13.56 MHz) and the tree-walking protocol (915 MHz). Juels [19] used this feature to propose a passive

jamming approach based on the tree-walking singulation protocol, called blocker tag. A blocker tag simulates the full spectrum of possible serial numbers for tags. In [17], Juels and Brainard propose a weaker privacy-protection mechanism, soft blocking. Soft blockers simply show the privacy preferences of their owners to RFID readers.

5.5 Bill of Rights

In [11], Garfinkel proposed a so-called RFID Bill of Rights that should be upheld when using RFID systems. He does not try to turn these rights into Law, but to offer it as a framework that companies voluntarily and publicly should adopt.

5.6 Classic Cryptography

1. ***Rewritable Memory***
   In 2003, Kinoshita [22] proposed an anonymous-ID scheme. The fundamental idea of his proposal is to store an anonymous ID, $E(\mathrm{ID})$, of each tag, so that an adversary can not know the real ID of the tag. E may represent a public or a symmetric key encryption algorithm, or a random value linked to the tag ID. In order to solve the tracking problem, the anonymous ID stored in the tag must be renewed by re-encryption as frequently as possible.
2. ***Symmetric Key Encryption***
   Feldhofer [10] proposed an authentication mechanism based on a simple two-way challenge-response algorithm. The problem with this approach is that it requires to have AES implemented in an RFID tag. In [21] we can find a state of the art on AES implementations in RFID systems.
3. ***Public Key Encryption***
   There are solutions that use public-key encryption, based on the cryptographic principle of re-encryption. The reader interested in the precise details can read the paper of Juels [18]. Other two interesting papers that tackle the subject of re-encryption are [12] and [28].

5.7 Schemes Based on Hash Functions

One of the more widely used proposals to solve the security problems that arise from RFID technology (privacy, tracking, etc.) is the use of hash functions.

1. ***Hash Lock Scheme***
   Weis [32] proposed a simple security scheme based on one-way hash functions. Each tag has a portion of memory reserved to store a temporary *metaID* and operates in either a locked or an unlocked state. The reader hashes a key k for each tag, and each tag holds a *metaID* ($metaID = hash(k)$). While locked, a tag answers all queries with his *metaID* and offers no other functionality. To unlock a tag, the owner queries the back-end database with the *metaID* from the tag, looks up the appropriate key and sends the key to the tag. The tag hashes the key and compares it to the stored *metaID*.

2. ***Randomized Hash Lock Scheme***
   One of the problems of the previous solution is that it allows the tracking of individuals. To avoid this, the *metaID* should be changed repeatedly in an unpredictable way. In order to solve this problem, Weis [32] proposed an extension of the hash lock scheme. It requires that tags have a hash function and a pseudo-random number generator.
3. ***Hash-Chain Scheme***
   Ohkubo, in [27], suggested a list of five points that must be satisfied in all security designs of RFID schemes: keep complete user privacy, eliminate the need for extraneous rewrites of the tag information, minimize the tag cost, eliminate the need for high power of computing units, and provide forward security. In [27], a hash-chain scheme was proposed, in which two hash functions (G and H) are embedded in the tag.

Some other recent published works on the use of hash functions are [6,7,14,23,34].

5.8 A Basic PRF Private Authentication Scheme

Molar [26] proposed a scheme for mutual authentication between tags and readers, with privacy for the tag. This protocol uses a shared secret s and a Pseudo-Random Function (PRF) to protect the messages exchanged between the tag and the reader.

5.9 Tree-Based Private Authentication and Delegation Tree

One of the main drawbacks of the hash schemes already proposed is that the load of the server (for identifying tags) is proportional to the number of tags. Molnar [26] has proposed a new scheme to reduce this load, which is named *Tree-Based Private Authentication*. This new protocol reduces the load to $O(\log n)$ but introduces the use of a Trust Center (TC). In order to reduce the burden on the TC, an offline delegation has been proposed [25]. Another interesting proposal is the work of Gildas and Oechslin [1], where a time-space trade-off is proposed.

5.10 Human Protocols

In [31], Weis introduced the concept of human computer authentication protocol due to Hopper and Blum, adaptable to low-cost RFIDs. This concept has been recently extended in an article by Weis and Juels [20], where they propose a lightweight symmetric-key authentication protocol named HB^+.

The security of both the HB and the HB^+ protocols is based on the *Learning Parity with Noise Problem*, whose hardness over random instances still remains as an open question.

5.11 Non-cryptographic Primitives

There are some solutions which do not use true cryptographic operations. The authors in [30] proposed a set of extremely-lightweight challenge-response authentication protocols. These protocols can be used for authenticating tags, but

they can be broken by a powerful adversary. In [16], Juels proposed a solution based on pseudonyms without using hash functions at all. The RFID tags store a short list of random identifiers or pseudonyms (known by authorized verifiers to be equivalent). When tag is queried, it emits the next pseudonym in the list.

6 Conclusions

RFID technology is one of the most promising technologies in the scope of ubiquitous computing. For it to become a reality, two kinds of problems must be solved: on one hand, *technological problems* and, on the other, *social problems*.

1. ***Technological Problems***
   Mark Weiser [33] (an early visionary of ubiquitous computing) announced (in 1991!) that one of the main problems that ubiquitous computing would have to solve was privacy. Deeply associated with it is the problem of tracking, or violations of location privacy.
   We have presented some of the most relevant solutions which try to address the fundamental security problems of RFID technology (privacy and tracking). Most of the proposed solutions rely on schemes based on the implementation of cryptographic hash functions in the tag. Although it is true that this could be possible in a short period of time, we consider that the current state of the art is still far from this point, so schemes based in hashing are not currently feasible. Alternatively, new lightweight hashing schemes especially suitable for RFID implementations, have not been scrutinized enough to be considered secure, a notable example is the ASHF used in SecurID [3].
2. ***Social Problems***
   Even considering that technological problems could eventually be solved, the implantation of RFID systems to a great scale will not be a reality if *we don't educate* people about their potential benefits, and if we cannot offer a guaranteed level of security. For example, a recent report [13] showed the numbers of a study made on *RFID and Perception of Control* pointing out that a 73.4% of those polled preferred to deactivate tags after buying a product. This clearly shows that, although advances in technological problems have been made, this is not yet reflected in the society, on the average citizen, which is, after all, who has the last word in deciding the future of a given technology.

References

1. G. Avoine and P. Oechslin. A scalable and provably secure hash-based RFID protocol. In *PERSEC'05*, pages 110–114. IEEE Computer Society Press, 2005.
2. C.A. Balanis. *Antenna theory: analysis and design*. John Wiley and Sons, 1997.
3. A. Biryukov, J. Lano, and B. Preneel. Recent attacks on alleged securid and their practical implications. *Computers and Security*, 24(5):364–370, 2005.
4. CASPIAN. http://www.nocards.org/, 2005.

5. Auto-ID Center. 900 MHz class 0 radio frequency (RF) identification tag specification. Draft, March 2003.
6. E.Y. Choi, S.M. Lee, and D.H. Lee. Efficient RFID authentication protocol for ubiquitous computing environment. In *Proc. of SECUBIQ'05*, LNCS, 2005.
7. T. Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proc. of SECURECOMM'05*, 2005.
8. GS1 - EAN International. http://www.ean-int.org/, June 2005.
9. EPCglobal. http://www.epcglobalinc.org/, June 2005.
10. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *Proc. of CHES'04*, volume 3156 of *LNCS*, pages 357–370, 2004.
11. S. Garfinkel. Bill of Rights. http://www.technologyreview.com, October 2002.
12. P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. In *CT-RSA'04*, volume 2964 of *LNCS*, pages 163–178. Springer-Verlag, February 2004.
13. O. Gunther and S. Spiekermann. RFID and the perception of control: the consumer's view. *Commun. ACM*, 48(9):73–76, 2005.
14. D. Henrici and P. Müller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In *PERSEC'04*, pages 149–153. IEEE Computer Society, 2004.
15. ITU page on definitions of ISM bands. http://www.itu.int/ITU-R/terrestrial/faq/index.html, September 2005.
16. A. Juels. Minimalist cryptography for low-cost RFID tags. In *SCN'04*, volume 3352 of *LNCS*, pages 149–164. Springer-Verlag, 2004.
17. A. Juels and J. Brainard. Soft blocking: Flexible blocker tags on the cheap. In *WPES'04*, pages 1–7. ACM, ACM Press, October 2004.
18. A. Juels and R. Pappu. Squealing euros: Privacy protection in RFID-enabled banknotes. In *FC'03*, volume 2742 of *LNCS*, pages 103–121. IFCA, Springer-Verlag, January 2003.
19. A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *ACM CCS'03*, pages 103–111. ACM, ACM Press, October 2003.
20. A. Juels and S. Weis. Authenticating pervasive devices with human protocols. In *CRYPTO'05*, volume 3126 of *LNCS*, pages 293–308. IACR, Springer-Verlag, 2005.
21. M. Jung, H. Fiedler, and R. Lerch. 8-bit microcontroller system with area efficient AES coprocessor for transponder applications. Ecrypt Workshop on RFID and Lightweight Crypto, 2005.
22. S. Kinoshita, F. Hoshino, T. Komuro, A. Fujimura, and M. Ohkubo. Low-cost RFID privacy protection scheme. In *IPS Journal 45, 8*, pages 2007–2021, 2003.
23. S.M. Lee, Y.J. Hwang, D.H. Lee, and J.I.L. Lim. Efficient authentication for low-cost RFID systems. In *Proc. of ICCSA'05*, volume 3480 of *LNCS*, pages 619–627. Springer-Verlag, 2005.
24. mCloak for RFID tags. *http://www.mobilecloak.com/rfidtag/rfid.tag.html*, September 2005.
25. D. Molnar, A. Soppera, and D. Wagner. A scalable, delegatable, pseudonym protocol enabling ownership transfer of RFID tags. Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
26. D. Molnar and D. Wagner. Privacy and security in library RFID: Issues, practices, and architectures. In *ACM CCS'04*, pages 210–219. ACM, ACM Press, October 2004.

27. M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic approach to "privacy-friendly" tags. In *RFID Privacy Workshop*, 2003.
28. J. Saito, J.-C. Ryou, and K. Sakurai. Enhancing privacy of universal re-encryption scheme for RFID tags. In *EUC'04*, volume 3207 of *LNCS*, pages 879–890. Springer-Verlag, August 2004.
29. W. Sean and L. Thomas. Automatic identification and data collection technologies in the transportation industry: BarCode and RFID. Technical report, 2001.
30. I. Vajda and L. Buttyán. Lightweight authentication protocols for low-cost RFID tags. In *UBICOMP'03*, 2003.
31. S. Weis. Security parallels between people and pervasive devices. In *PERSEC'05*, pages 105–109. IEEE Computer Society Press, 2005.
32. S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Security in Pervasive Comp.*, volume 2802 of *LNCS*, pages 201–212, 2004.
33. M. Weiser. The computer for the 21st century. *Scientific American*, 265(3):94–104, September 1991.
34. J. Yang, J. Park, H. Lee, K. Ren, and K. Kim. Mutual authentication protocol for low-cost RFID. Ecrypt Workshop on RFID and Lightweight Crypto, 2005.

TMSI Allocation Mechanism Using a Secure VLR Authorization in the GSM System

Mi-Og Park[1], Dea-Woo Park[2], and Sang-Geun Kim[1]

[1] Division of Computer Engineering, Sungkyul University, San 142-7, Manan-gu, Anyang 8-dong, Anyang-city, Gyeonggi-do, Korea 430-742
Mopark777@hanmail.net, Sgkim@sungkyul.edu
[2] Department of Computer Science, Soongsil University, Sangdo-dong 511, Donggak-gu, Seoul, Korea 156-743
Prof1@hanmail.net

Abstract. GSM is the most popular standard for mobile phones in the world. In spite of the tremendous market growth, however, the GSM system has the fatal security problems in TMSI allocation protocol. These problems are right user authentication and location privacy. In this paper, we propose the secure TMSI allocation mechanism using the certification concept to solve these problems. The proposed mechanism provides partial anonymity, which has been rarely provided in the other approaches. Also we propose the modified mechanism to reduce TMSI allocation procedure without changing of the architecture of the original GSM system.

1 Introduction

The Global System for Mobile Communications (GSM) is the most popular standard for mobile phones in the world. GSM service is used by over 1.5 billion people across more than 210 countries and territories. The ubiquity of the GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. GSM is an open standard which is currently developed by the 3GPP[1]. Security in GSM consists of the following aspects: subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. The subscriber is uniquely identified by the International Mobile Subscriber Identity (IMSI). This information, along with the individual subscriber authentication key Ki, constitutes sensitive identification credentials analogous to the Electronic Serial Number (ESN) in analog systems such as AMPS and TACS. The design of the GSM authentication and encryption schemes is such that this sensitive information is never transmitted over the radio channel. Rather, a challenge-response mechanism is used to perform authentication. The actual conversations are encrypted using a temporary, randomly generated ciphering key (Kc). The Mobile Station (MS) identifies itself by means of the Temporary Mobile Subscriber Identity (TMSI), which is issued by the network and may be changed periodically for additional security[2].

When the MS roams from one place to another, it is verified by using these security functions. However, GSM has the major security weakness during this procedure.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 171 – 181, 2006.

The fatal problem is that anyone can listen an authentication parameter IMSI, which is uniquely identified a MS. In order to solve the problems with the TMSI allocation protocol in GSM, a lot of mechanisms have been proposed [3][4][5][6][7]. The most common mechanisms for secure TMSI allocation use basically the encryption between the VLR and the HLR. And also there are the many mechanisms that use the VLR authorization, which means that the VLR instead of the HLR authenticates the legality of the MS. In this paper, our mechanisms basically use the security functions, too. However, our mechanisms additionally provide the more many advantages than the existed ones.

The rest of the paper is organized as follows: First, we describe the TMSI allocation protocol defined in GSM. Then, we briefly describe the security of GSM e.g., user authentication and data confidentiality and the problems with TMSI allocation protocol in GSM. The main focus of the paper is Section 3, which propose the secure TMSI allocation protocol to solve the problems addressed above. In Section 4 and 5 we explain the main features and cryptanalysis about the proposed mechanism. We finally conclude this paper with a brief summary.

2 TMSI Allocation in GSM

2.1 Security Functions: Authentication and Confidentiality

In the GSM network, the subscriber is initially registered in the HLR with a unique identity, IMSI, and obtains one secret key Ki from the AuC(Authentication Center) during the registration process. HLR is a database used for mobile information management. All permanent subscriber data are stored in this database. The VLR is the database of the service area visited by an MS. Two location databases play important roles in subscribers' registration and authentication[8].

• User Authentication

Authentication is initiated by the fixed network, and is based upon a simple challenge-response protocol. When a MS attempts to access the system, the network issues it a 128-bit random challenge RAND. The MS computes the 32-bit signed response (SRES) based on the encryption of the random number RAND with the authentication algorithm (A3) using the individual subscriber authentication key Ki. The key Ki is unique to the subscriber, and is shared only by the subscriber and an authentication center, which serves the subscriber's home network. The value SRES computed by the MS is signaled to the network, where it is compared with a pre-computed value. If the two values of SRES agree, the mobile subscriber has been authenticated, and the call is allowed to proceed. If the values are different, then access is denied. The subscriber authentication key is never transmitted over the radio channel. It is present in the subscriber's SIM, as well as the HLR and VLR databases[9][10].

• Data Confidentiality

The same mechanism is also used to establish a cipher key Kc for encrypting user and signaling data on the radio path. This procedure is called cipher key setting in [3]. The key is computed by the MS using a one-way function A8, again under control of the subscriber authentication key, and is pre-computed for the network by the

authentication center, which serves the subscriber's home network. Thus at the end of a successful authentication exchange, both parties possess a fresh Kc. The Kc is used to encrypt and decrypt the data between the MS and the VLR. The pre-computed triple (RAND, SRES, Kc) held by the fixed networks for a particular subscriber is passed from the home network's authentication center to visited networks upon demand. The challenges are used just once. Thus the authentication center never sends the same triple to two distinct networks, and a network never re-uses a challenge.

In a similar manner to the authentication process, the computation of the ciphering key takes place internally within the SIM. Therefore sensitive information such as the individual Ki is never revealed by the SIM. Encrypted voice and data communications between the MS and the network are accomplished through use of the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the A5 and the Kc.

2.2 TMSI Allocation

The TMSI allocation allows mobile subscribers to originate calls and update their location without revealing their IMSI to an eavesdropper on the radio path. It thus prevents location tracing of individual mobile subscribers by listening to the signaling exchanges on the radio path. All mobiles and networks must be capable of supporting the service, but its use is not mandatory.

• TMSI Allocation Protocol and Its Problems

The TMSI updating mechanism functions in the following manner. For simplicity, assume the MS has been allocated a TMSI, denoted by $TMSI_o$, and the network knows the association between $TMSI_o$ and the subscriber's IMSI. The MS identifies itself to the network by sending $TMSI_o$. Immediately after authentication, the network generates a new TMSI, denoted $TMSI_n$, and sends this to the MS encrypted under the Kc as described in the above section. Upon receipt of the message, the MS deciphers and replaces $TMSI_o$ by $TMSI_n$[10].

Since GSM does not adopt ciphering mechanism between the VLR and VLR/HLR, an eavesdropper can monitor the physical channel that connects to the HLR. Also he can eavesdrop MS's location updating and user authentication information. These drawbacks of GSM enlarge the possibility of the privacy violation on users. It is found that the TMSI allocation protocol has some problems and weaknesses as follows[8]. The most important problem is the exposure of the IMSI and some other things are weakness.

• When the VLR updates the location of the MS, the IMSI is exposed and delivered throughout the network without any protection. This is the big problem in user authentication protocol.

• Mutual authentication mechanism between the MS and the VLR isn't provided. The GSM system only provides unilateral authentication for the MS. Using the challenge and response mechanism, the identity of a MS is verified. However, the identity of the VLR cannot be authenticated. It is therefore possible for an intruder to pretend to be a legal network entity and thus to get the MS' credentials.

• The VLR must turn back to the HLR to make a request for another set of authentication parameters when the MS stays in the VLR for a long time and exhausts its set of authentication parameters for authentication. There is bandwidth consumption between the VLR and the HLR.

• Every MS in the VLR has n copies of the authentication parameters. The parameters are stored in the VLR database, and then space overhead occurs.

• Authentication of the MS is done in the VLR and this must be helped by the HLR of the MS for each communication.

• When a user roams to another VLR, the location is updated by sending IMSI to the new VLR while the old VLR is not accessible and no correct subscriber data is available. It is possible that an unauthenticated third party may eavesdrop on the IMSI and identify this mobile user.

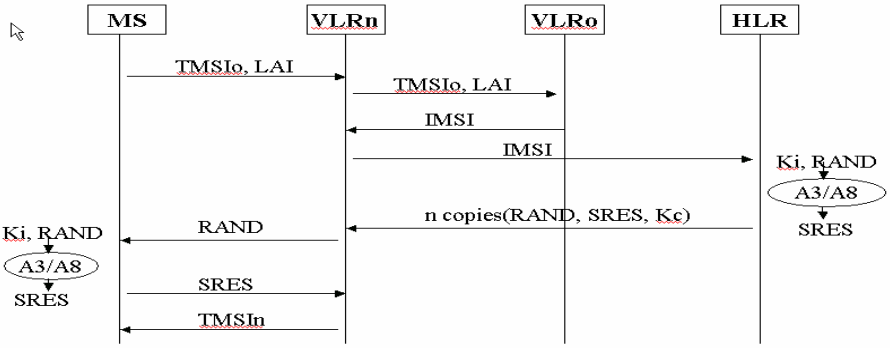


Fig. 1. TMSI Allocation Protocol and Security Functions

3 Secure TMSI Allocation Protocol

3.1 Basic Principles

The proposed mechanism will achieve the following main design objectives: secure user authentication, location privacy, partial anonymity, secure distribution of IMSI, the VLR authorization, and secure communication between the VLR and the HLR. Also the proposed mechanism has the following additional objectives: mutual authentication, reduction of the stored space in the VLR, and reduction of bandwidth consumption between the VLR and the HLR.

• The Generation Method of TID

Our mechanism provides the partial anonymity capability. However, the most common papers seldom provide user's anonymity[3][8]. In this paper, partial anonymity has literally the meaning that guarantees partially user anonymity in the TMSI allocation protocol. In order to provide partial anonymity, the proposed mechanism uses a MS's temporary identity (TID). The usage of a TID can also avoid the location tracking. The old VLR transmits the TID instead of the IMSI to the new VLR before completing verification of the new VLR by the HLR. The new VLR can acquire the IMSI

only after being completed verification by the HLR. So user's anonymity is provided until the new VLR is authenticated by the HLR.

The TID is mapped by one-to-one with the IMSI. So the TID must be unique in the HLR of the MS as an additional parameter to authenticate the MS instead of the IMSI. The relation between the TID and the IMSI is kept secretly only by the HLR and the MS. But, the parameter TID itself is public information. And only the HLR can generate user's new TID. User can take together new TID during the registration process that he/she obtains the Ki and the IMSI. The HLR gives the new VLR authorization to authenticate the MS. But, the new VLR processes authentication of the MS without knowing the Ki of the MS. If the MS stays in the coverage of its new VLR for a long time, the new VLR does not go back to the HLR to require another set of authentication triple (RAND, SRES, Kc) to authenticate the MS.

• The Generation Method of the Certificates

The VLR authorization means the capability that the new VLR instead of the HLR authenticates the MS. For this capability, the new VLR must have a temporary secret key shared between itself and the HLR. We notate this key as a TKi. The new VLR only uses the TKi of the HLR given with its generated RANDj for each call to compute the SRES and then identifies the MS, where RANDj is a random number generated by the new VLR in the subsequent calls. Only one RANDj is generated by the new VLR for each jth call no matter how long the MS stays in the coverage of the new VLR. This operation will be done only once in the first call when the MS visits at the new VLR.

Table 1. Notations

T1	Timestamp generated by the MS
T2	Timestamp generated by the new VLR
RAND1, RANDv	Random numbers generated by the new VLR
RAND	Random number generated by the HLR
K_{VH}	Secret key shared between the HLR and the VLR

In order to endow the new VLR with MS authorization, the HLR requires legality of the new VLR. We use the certification concept to check legality of the new VLR. The HLR generates the certification of the VLR e.g., $Cert_{HM}$ after performing authentication of the VLR. In our paper, the certifications ($Cert_{HM}$, $Cert_{MS}$, and $Cert_{VLR}$) are different from the general certification in a public key infrastructure cryptosystem. The MS computes the certification of the MS, $Cert_{MS}$ through A3 using (Ki, T1) to prove itself to the HLR. In order to obtain the capability that authenticates the MS from the HLR, the new VLR should be strongly verified by the HLR. The compositions of the VLR certification e.g., $Cert_{VLR}$ are K_{VH}, RANDv, T1, and T2. $Cert_{VLR}$ is generated by running A3 using K_{VH} and X3, which is produced by computation of XOR with T1, T2, and RANDv.

The HLR computes the certification of the new VLR, e.g., $Cert_{HM}$ through A3 using (Ki, T1) and (Ki, RAND) to prove the fact that the new VLR is a genuine entity to the MS. The temporary key between the MS and the new VLR, TKi is computed by running A3 with Ki and the result value after doing XOR RAND and T1.

Table 2. Certification Generation Method

$Cert_{MS}$	A3(Ki, T1)
$Cert_{VLR}$	A3(K_{VH}, X3)
$Cert_{HM}$	A3(Ki, T1) ‖ A3(Ki, RAND)

3.2 TMSI Allocation Procedure

The procedure for the proposed TMSI allocation mechanism is following as:

Step 1) The MS sends TMSI, LAI, $Cert_{MS}$, TID, and a time-stamp T1 to the new VLR. T1 enables to authenticate the new VLR and it prevents from replay attack.

Step 2) After receiving TMSI and LAI, the new VLR forwards TMSI and LAI to the old VLR to obtain the MS's TID.

Step 3) The old VLR sends the TID instead of IMSI to the new VLR after searching for the TID corresponding to TMSI and LAI in its database. If there is no TID corresponding to the TMSI and LAI, then the session will be terminated.

Step 4) The new VLR generates RANDv and timestamp T2. And then the VLR computes $Cert_{VLR}$ according to the certification generation method. After that, the VLR transmits the TID along with the identity of the VLR, e.g., VLR_{ID}, T1, T2, RANDv, $Cert_{MS}$ and $Cert_{VLR}$ to the HLR. RANDv and T2 are used to authenticate the VLR itself to the HLR. RANDv may be encrypted using A5 with Kvh for the secure transaction, since the RANDv is used as the parameter to authenticate the VLR in the HLR.

Step 5) Once receiving the parameters, the HLR checks if VLR_{ID} is a legal or not. If it is correct, then the HLR computes the X3 by using the transmitted T1, T2, and RANDv and does $Cert_{VLR}$' value to authenticate the VLR, since the HLR knows the shared key K_{VH} between the VLR and the HLR corresponding to the VLR_{ID}. If $Cert_{VLR}$' and $Cert_{VLR}$ are same, the HLR believes the new VLR is a genuine entity and computes TKi. And then the HLR computes Evh(IMSI, TKi) through A5 with a secret key K_{VH} using the TKi and the IMSI corresponded to the transmitted TID. At the same time, the HLR generates RAND and computes E_{HM}(RAND) using A5 and $Cert_{HM}$. Finally, the HLR transmits the identity of the HLR e.g., HLR_{ID}, T1, $Cert_{HM}$, E_{HM}(RAND), and E_{VH}(IMSI, TKi) to the new VLR.

Step 6) Once receiving the parameters, the new VLR extracts the IMSI and the TKi, since it can know the shared secret key K_{VH} by checking the HLR_{ID}. The VLR generates the random number RAND1 to authenticate the MS. In the next call, the VLR should generate another random number. The VLR transmits T1, E_{HM}(RAND), RAND1, and $Cert_{HM}$ to the MS.

Step 7) Upon receiving the parameters, the MS first checks if T1 is the same as it was when last sent. If the result is valid, the MS computes $Cert_{HM}$' and then it compares the $Cert_{HM}$' computed by itself with the $Cert_{HM}$ received from the VLR. If two certification values are the same, the MS believes the new VLR and generates TKi after decryption E_{HM}(RAND). The MS continues through A5 using TKi and RAND1 as inputs to generate the SRES, which is then sent back to the new VLR.

Step 8) Once receiving the SRES from the MS, the new VLR computes the SRES' through A3 using TKi and RAND1 and compares the SRES' with the received SRES.

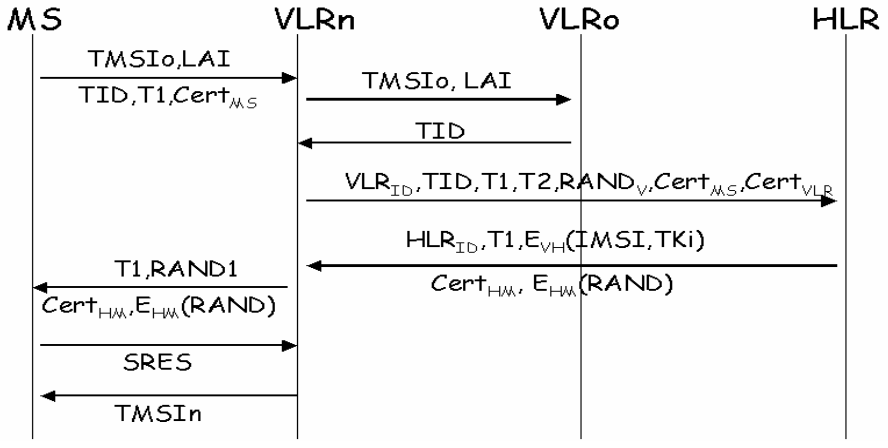


Fig. 2. Secure TMSI Allocation Procedure

If they are the same, the authentication of the MS is successful. Finally, the new VLR generates and transmits the new TMSI to the MS.

3.2 The Reduction of Procedure

In order to reduce the numbers of the proposed procedure, we introduce the modification mechanism that changed the procedure of the first proposed mechanism. The basic concepts are the same as one of the first proposed mechanism. However, there is one different point in the procedure.

One difference is that steps 2 and 4 in the first mechanism are simultaneously performed in the second mechanism. So, steps 3 and 5 are automatically and simultaneously performed after being completed them respectively. That is to say, the new VLR immediately transmits the TID that is sent from the MS to the HLR after completing the 1st step without waiting for the transmission of the TID from the old VLR in the 3rd step because the new VLR already has the TID that sent from the MS in the 1st step. As a result of, steps 2 and 4 in the first mechanism become step 2 in the second one. And steps 3 and 5 in the first mechanism become step 3 in the second one.

4 Main Features

Our mechanisms provide the following features. So our mechanisms satisfy the design objectives. First, we explain the features that provided in only our mechanisms.

• The first user authentication and the second one: In step 3 of the first proposed mechanism, the new VLR can know that certain attack exists if the different TID is sent from the old VLR. Thus, the first proposed mechanism provides the first user authentication to authenticate simply the MS by the transmission of the TID in step 3. The second user authentication is provided in step 5, which is the core user authentication. In our second mechanism, the first user authentication and second one are provided in step 3. Steps 3 and 5 of the first mechanism belong to step 3 of the second

mechanism because of the simultaneous processing character of the second mechanism. Thus the proposed mechanisms provide the feature that can authenticate the MS two times without the additional procedures.

• Partial anonymity: The conventional mechanisms don't provide almost partial anonymity. Our mechanisms provide the mobile user with partial anonymity by using a TID until the HLR of the MS authenticates the new VLR. The procedure to provide partial anonymity brings the effect to reduce encryption processing, since the parameter TID itself is the public information in our paper.

• Stronger VLR authentication: The proposed mechanisms provide the stronger VLR authentication. In the common mechanisms for the secure TMSI allocation, the original user authentication of the GSM system has been used to authenticate the new VLR by the HLR. That is to say, the HLR authenticates the new VLR by using the A3 with a Ki and a time-stamp T in the common mechanisms. However, in the system that the new VLR instead of the HLR authenticates the MS, it's necessary the more secure authentication function to authenticate the new VLR because the new VLR is responsible for the MS authentication. Our VLR authentication method is more secure for the additional VLR authentication parameters as described in section 3.

• Only VLR that is authenticated by HLR can use MS's IMSI: The conventional mechanisms and the original GSM system assume that the VLR is a legal entity. But, in this paper, the HLR believes the new VLR according to the verification result after authenticating the new VLR without any assumption. By the certification generation method of the new VLR, the HLR can authenticate securely the new VLR.

• Procedure reduction: The second proposed mechanism reduces from 8 to 6 steps for a new TMSI allocation and from 7 to 5 steps for the MS authentication in the new VLR because of the simultaneous processing of the second mechanism. So our mechanism can authenticate the MS and allocate the new TIMSI in shorter time. Also it reduced the total procedure without totally changing the original architecture of GSM.

The following items are features that have been provided in the most common approaches for secure TMSI allocation. Our mechanisms also provide the following features.

• Secure user authentication and location privacy: These are the most important objective. Our mechanism used the TID instead of the IMSI between the new VLR and the old VLR. It is possible for any network entities including the new VLR to acquire the IMSI only after the HLR of the MS authenticates them. When the HLR transfer the IMSI to the new VLR, the IMSI is sent in the encrypted mode by using the shared secret key between the HLR and the VLR. Thus user authentication and location privacy are supported, since the value IMSI isn't exposed the unauthenticated entities.

• Mutual authentication between the MS and the VLR: The HLR generates the $Cert_{VLR}$ after authenticating the new VLR by the $Cert_{VLR}$. By verifying the $Cert_{VLR}$ transmitted from the HLR, the MS can ensure that it is communicating with a legitimate VLR.

• Reduction of bandwidth consumption: The HLR gives the VLR temporary secret key TKi to authenticate the MS. As long as the MS stays in the coverage area of the new VLR, the VLR can use the TKi to authenticate the MS for each call. Since the

new VLR does not go back to the HLR to require another set of authentication triple, the signaling load is reduced between the VLR and the HLR.

• Reduction in the storage of the VLR database: The VLR only stores one authentication parameter instead of n copies (RAND, SRES, Kc) according to the principle of the reduction of bandwidth consumption.

• The application of the existed security: There is no any change in the original architecture in order not to lose simplicity and efficiency advantages of GSM, which is widespread in the world. The security of the proposed mechanisms is also still based on algorithms A3, A5 and A8.

• Authentication of the MS by the new VLR: Authentication of the mobile user is to be done by the new VLR instead of the HLR except the first call for the TMSI allocation, even though the VLR doesn't know the subscriber's secret key Ki.

The conventional approaches don't satisfy all our design objectives. And also the many approaches mostly change the original architecture of the GSM TMSI allocation protocol. Our mechanisms keep the advantage of not changing the architecture of the GSM system. Table 3 shows some approaches with the unchanged architecture. Lee et al. [8] proposed a mechanism that doesn't change the architecture. But, their mechanism doesn't provide mutual authentication between the MS and the VLR. The original GSM doesn't also support mutual authentication. Since the VLR doesn't ask the HLR for another set of authentication triple in Lee et al.'*s* and our mechanisms, the bandwidth consumption is less than that of the original GSM protocol. Because the VLR only requires storage of one copy of the authentication triple instead of n copies in Lee et al.'s and our mechanisms, the storage in the VLR can be saved.

The explained capabilities are concisely arranged in table 3. The followings are the meanings of the abbreviated words: PA: Partial anonymity, AI: Assignment of the IMSI, UAV: The use of IMSI after authentication the VLR, EVV: Encryption between the old VLR and new VLR, RBC: Reduction of bandwidth consumption, RSV: Reduction of storage in the VLR, RTP: Reduction of the total procedure, MAMV: Mutual authentication between the MS and the VLR, CAG: Change architecture of GSM. As shown in table 3, the common approaches have used encryption between the old VLR and the new VLR. Also they encrypted all parameters between the VLR and the HLR. However, the proposed mechanisms made to the minimum the usage of encryption by applying it to the only parameters is in need of encryption.

Table 3. Comparison among TMSI allocation mechanisms

	GSM	Our mechanism	[8]	[7]	[11]
PA	N	Y	N	N	N
AI	VLR	HLR	VLR	VLR	VLR
UAV	N	Y	N	N	N
EVV	N	N	Y	Y	Y
RBC	N	Y	Y	N	Y
RSV	N	Y	Y	N	Y
RTP	-	N	Y	Y	N
MAMV	N	Y	N	Y	N
CAG	-	N	N	N	N

5 Cryptanalysis

Owing to the fact that we adopt the architecture of the conventional authentication in GSM, the security of the proposed mechanisms, which is the same as that of the existing authentication method in GSM, is based on algorithms A3, A5 and A8. In order to authenticate the legality of the new VLR and the MS, we add a time-stamp T1 and T2 to the TMSI allocation protocol. The T1 and T2 enhance the security of the proposed mechanisms against a replay attack. Although an attacker can intercept T1, T2, RANDv and $Cert_{VLR}$ and then forge the real VLR, the replay still cannot succeed because T1 and T2 are incorrect. The MS can also check if the T1 is the same as it was when sent the last time even if the fake VLR replays T1 and $Cert_{VLR}$.

The new VLR is verified in the MS by using the $Cert_{HM}$ that generated from the HLR. Nobody can forge it to fool others, since the secret key Ki is known only to the MS and the HLR. The proposed $Cert_{HM}$ and $Cert_{VLR}$ are made the stronger than the other certification mechanisms of the new VLR. Without the knowledge of Ki, $Cert_{HM}$ cannot be computed by anyone. Therefore, the security of the proposed mechanisms is based on Ki. For authenticating the MS, the new VLR only generates a different RANDj to compute the SRES for every jth call. The security here is based on the HLR giving the new VLR authorization to authenticate the MS. Nobody can suppose the value IMSI with the TID, since only the HLR knows the relation between the TID and the IMSI. Also there is no the exposure of the IMSI in wired channel, since the only authenticated VLR can use the IMSI and this VLR is transfer the IMSI in encryption mode.

6 Conclusions

In this paper, we have proposed new TMSI allocation mechanisms used the certification concept to solve the fatal problems of user authentication and location privacy in the GSM system. Besides, the proposed mechanisms provide partial anonymity and stronger VLR authentication. The stronger VLR authentication is very important in the most common approaches for the secure TMSI allocation, which have used the way that the new VLR instead of the HLR authenticates the MS. In order to authenticate the MS by the new VLR instead of the HLR, the HLR must strictly authenticate the new VLR. Thus the stronger VLR authentication is needed. However, the most approaches have merely used the general user authentication of the original GSM system. Our mechanisms provide the more secure way to authenticate the MS by the new VLR, since our approaches provide the stronger VLR authentication by applying the certification as described above. Also our mechanism provides the reduction of the TMSI allocation procedure by doing simultaneously the procedure without changing the procedures of the original GSM system.

References

1. http://en.wikipedia.org/wiki/GSM
2. http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html
3. HARN, L. and LIN, H.Y: Modification to enhance the security of the GSM protocol, Proceedings of the 5th National Conference on Information security, Taipei, Taiwan, May. (1995) 416-420

4. Lee C.C., Hwang M.S., Yang, W.P.: Extension of authentication protocol for GSM. IEE Proceedings. Communications, Vol. 150, No.2, (2003) 91-95
5. AL-TAWIL, K., AKRAMI, A., and YOUSSEF, H.: A new authentication protocol for GSM networks, Proceedings of IEEE 23rd Annual Conference on Local computer networks(LCN'98), 21-30 (1998)
6. STACH, J.F., PARK, E.K., and MAKKI, K.: Performance of an enhanced GSM protocol supporting non-repudiayion of service, Comput. Commun., 675-680 (1999)
7. Molva, R., Samfat, D., Tsudik, G.: Authentication of mobile users, Network, IEEE Volume 8, Issue 2, (1994) 26 – 34
8. K. Chae and M. Yung (Eds.): WISA 2003, LNCS 2908, pp. 162.173, 2004. Springer-Verlag Berlin Heidelberg 2004, A Location Privacy Protection Mechanism for Smart Space
9. http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsmsecur.html
10. http://jya.com/gsm061088.htm
11. Chii-Hwa Lee, Min-Shiang Hwang and Wei-Pang Yang, Enhanced privacy and authentication for the global system for mobile communications, Wireless Networks 5 (1999) 231–243

On the Anomaly Intrusion-Detection in Mobile Ad Hoc Network Environments

Ricardo Puttini[1], Maíra Hanashiro[1], Fábio Miziara[1],
Rafael de Sousa[1], L. Javier García-Villalba[2,*], and C.J. Barenco[3]

[1] Universidade de Brasília (UnB), Campus Universitário Darcy Ribeiro,
Faculdade de Tecnologia, Depto. de Engenharia Eléctrica, Laboratório de Redes – sala B1
CEP: 70910-900, Brasília – DF - Brazil
University of Brasília, Brazil
{puttini, desousa}@unb.br, {maira, fabimiziara}@redes.unb.br
[2] Grupo de Análisis, Seguridad y Sistemas (GASS)
Departamento de Sistemas Informáticos y Programación (DSIP)
Facultad de Informática, Despacho 431
Universidad Complutense de Madrid (UCM)
C/ Profesor José García Santesmases s/n,
Ciudad Universitaria, 28040 Madrid, Spain
javiergv@sip.ucm.es
[3] Departamento de Computación y Tecnología de la Información
Universidad Simón Bolívar (USB)
Oficina MYS 213-B, Apartado Postal 89.000
Caracas, 1080 Venezuela
barenco@ldc.usb.ve

Abstract. Manet security has a lot of open issues. Due to its characteristics, this kind of network needs preventive and corrective protection. In this paper, we focus on corrective protection proposing an anomaly IDS model for Manet. The design and development of the IDS are considered in our 3 main stages: normal behavior construction, anomaly detection and model update. A parametrical mixture model is used for behavior modeling from reference data. The associated Bayesian classification leads to the detection algorithm. MIB variables are used to provide IDS needed information. Experiments of DoS and scanner attacks validating the model are presented as well.

1 Introduction

Security of Mobile Ad Hoc Networks (MANET) is an active topic in recent research. Most of current work on Manet security focuses on some kind of preventive protection design (e.g. authentication [1]). However, as network entities in a Manet consist of general-purpose hardware and software equipments, usually without good physical protection, occurrence of malfunctioning and compromised entities in such networks

* This work was partially supported by the Spanish Ministry of Education and Science (MEC) under Project TSI2005-00986.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 182 – 193, 2006.

cannot be neglected. Therefore, security must be designed in a way that the network service remains robust even in presence of misbehaving nodes. In general treat models, the compromising of a network entity leads to revealing all confidential information to the intruder, which allows for most of preventive security mechanisms to fail. Intrusion detection and response systems (IDS) are a common approach in such scenarios where a corrective security mechanism is required to cope with the limitations of preventive-only security mechanisms.

In respect to the IDS design, two basic approaches can be considered: misuse and anomaly intrusion detection. In misuse detection, an attack signature must be explicitly provided, leading to a positive identification of an attack occurrence. If the source of the attack (e.g. compromised node) can also be identified as part of the detection process, a simple corrective (response) action consists in excluding the attacker node from the network. This is the case for security systems based on the preventive and corrective protection by combination of strong authentication and misuse IDS [2]. Anomaly detection has a completely different base. The current behavior of the monitored system (e.g. network) is repeatedly compared with some reference behavior, which is previously stated (normal behavior). In this case, as existence of attacks is not explicitly realized, the problem source cannot be precisely identified. Thus, corrective (response) actions must concentrate on mitigation of attack effect.

In this paper, we propose the design of an IDS following the anomaly detection approach. We are especially interested in detecting anomalous network traffic behavior due to packet flooding (e.g. DoS) and scan attacks in mobile ad hoc networks.

Our first contribution is the presentation of an anomaly IDS conception. This design is based on statistical modeling of reference behavior using mixture models [3] in order to cope with an observable traffic composed by mixture of different traffic profiles due to different network applications. The detection algorithm is based on Bayesian classification criteria.

The second contribution is the adaptation on the statistical model in order to model network traffic behavior in Manet. Standard MIB variables are used as observations of the traffic behavior (during reference model establishment and detection). Simulations with ns-2 are conducted in order to validate this approach.

The remaining of this paper is organized as follows: Section 2 gives an overview of related works. Section 3 presents the anomaly IDS design. Section 4 presents the Manet traffic characterization and defines the behavior model construction. Finally, section 5 presents our conclusions and proposed future works.

2 Related Work

The IDS project for Manet is not a complete new issue and this subject has already been treated recently. Y. Zhang and W. Lee [4] introduce the basic requisite for this special kind of IDS. This architectural design was explored in V. Mittal and G. Vigna [5] who present an IDS formed by various sensors to detect attacks against the routing protocol that monitors promiscuously the network links. In a previous work, R. Puttini *et al.* [6] present the design of a fully-distributed IDS architecture.

In [7], G. Vigna *et al.* proposes an IDS for Manet that is essentially projected to reinforce the security of the routing protocol. In [2], Puttini R *et al.* propose a new security model for protection of Manet routing protocol. The salient features in this design are: combination of preventive and corrective protection, self-organized conception of security services and fully localized solutions. In the work at [8] it is presented a security solution based in a modified version of AODV that uses a mechanism of intrusion detection combined with a token system that is used to grant the node access to the routing services. However, this solution does not incorporate any preventive solution (authentication).

Y. Huang et al. [9] and C.-Y.Tseng et al. [10] present projects of IDS for Manet based on detection by anomaly strategy. Finally, a strategy of detection and response to intrusion to deal with non-cooperative nodes in ad hoc networks is presented by S. Marti et al. [11].

In this paper we present a completely new anomaly IDS design, based on statistical models for detecting DoS and scan attacks in Manet networks.

3 Anomaly IDS Design

This section presents our anomaly IDS model [3]. The idea is to build a behavior model that takes into account multiple use profiles and allows *a posteriori* Bayesian classification of data as part of the detection algorithm. A reference audit data set representing the normal system behavior is used to create the model with a learning procedure[1].

Before starting to describe the model, we should note that audit data must be mapped into random variables (e.g. into a number-based domain). Hereafter, we admit that audit data can be represented by a set of realizations of a continuous random vector **y**, which probability distribution function (pdf) will be modeled[2].

A. Behavior Model

Parametrical Mixture Model and EM-Algorithm

In our behavior model, the pdf of the (d-dimensional) random vector **y**, whose realizations are mapped from the audit data domain, are represented by a parametrical mixture model [12]. The mixture model fundamental equation, giving the probability of $\mathbf{y}_i$, can be formally expressed as:

$$p(\mathbf{y}_i) = \sum_{k=1}^{K} p(z_k) g_k(\mathbf{y}_i, \boldsymbol{\theta}_k) \cdot \tag{1}$$

[1] Obtaining good initial reference information set is not straightforward as assuring a data set to be representative for every expected behavior is usually difficult.

[2] Some data types are numerical by nature and are easily mapped. In this paper we admit input (reference and activity) data to be numerical, continuous and unbounded. This is not the case for every data type founded in real systems and special mapping and distributions are need when dealing with non-numerical, non-continuous or bounded data.

Where: yi is the i-th observed data; z is the hidden vector that indicates which source (profile) data comes from (e.g. zk = 1 if data comes from cluster k and z = 0, otherwise); gk are kernel distribution functions with respective parameters θk, each of them modeling one of the use profiles; K is the model order corresponding to the number of sources being modeled.

The unknown parameters in the model (Equation (1)) are the set of cluster probabilities ($p(z_k)$) and the parameters of kernel distribution functions of each cluster ($\boldsymbol{\theta}_k$), represented by $\boldsymbol{\Psi} = [p(z_1), p(z_2),..., p(z_k), \boldsymbol{\theta}_1, \boldsymbol{\theta}_2,..., \boldsymbol{\theta}_k]$. An iterative algorithm of optimizing the unknown vector $\boldsymbol{\Psi}$ by a maximum likelihood (ML) criterion has been defined and is called the expectation-maximization (EM) algorithm [13]. We let $\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2,..., \mathbf{y}_n]^T$ be an observed n-dimensional realization vector of $\mathbf{y}$ (which we like to model). $\mathbf{Y}$ is regarded as the reference data containing representative normal behavior information and are used to fit $\boldsymbol{\Psi}$ using the EM algorithm. This algorithm permits both log-likelihood and model parameter estimation to be done in an iterative manner. A detailed discussion of the EM-algorithm is out of the scope of this paper. The reader is asked to refer to [3,4] for a more general description of the EM-algorithm.

In the particular case of Gaussian mixture models (GMM), the Equation (1) should be rewritten replacing the general distrbutions (g_k) by the normal distribution (represented by ϕ) and the distribution parameters $\boldsymbol{\theta}_k$ by the mean vector ($\boldsymbol{\mu}_k$) and covariance matrix ($\mathbf{R}_k$), as stated at Equation (2), where the probabilty $p(z_k)$ are also replaced by the pondering factor w_k, for simplicity of notation.

$$p(\mathbf{y}_i) = \sum_{k=1}^{K} w_k \phi(\mathbf{y}_i, \boldsymbol{\mu}_k, \mathbf{R}_k) \tag{2}$$

For completeness, we provide the EM recursion equations (Equations (3)-(6)) for the Gaussian mixture models:

$$p(k \mid \mathbf{y}_i) = \frac{w_k^i \phi(\mathbf{y}_i, \boldsymbol{\mu}_k^i, \mathbf{R}_k^i)}{\sum_{k'=1}^{K} w_{k'}^i \phi(\mathbf{y}_i, \boldsymbol{\mu}_{k'}^i, \mathbf{R}_{k'}^i)} \tag{3}$$

$$w_k^{i+1} = \sum_{i=1}^{n} p(k \mid \mathbf{y}_i)/n \tag{4}$$

$$\boldsymbol{\mu}_k^{i+1} = \sum_{i=1}^{n} p(k \mid \mathbf{y}_i)\mathbf{y}_i / \sum_{i=1}^{n} p(k \mid \mathbf{y}_i) \tag{5}$$

$$\mathbf{R}_k^{i+1} = \sum_{i=1}^{n} p(k \mid \mathbf{y}_i)(\mathbf{y}_i - \boldsymbol{\mu}_k^{i+1})(\mathbf{y}_i - \boldsymbol{\mu}_k^{i+1})^T / \sum_{i=1}^{n} p(k \mid \mathbf{y}_i) \tag{6}$$

Optimal Entropy-Based Estimation of Model Order

For the propose of the EM-algorithm, the model order K must be provided because it is useful to be able to estimate the most probable number of partitions.

As described in [14], this "ideal partitioning" should be obtained by minimizing Shannon entropy given observed data, which can be evaluated for each observation by Equation (7):

$$H_K = -\sum_{k=1}^{K} p(k \mid \mathbf{y}_i) \log(p(k \mid \mathbf{y}_i)) \tag{7}$$

The expected value of this entropy is evaluated taking the mean of H_K over all observed data[3] (Equation(8)):

$$E^*(H_K) = -\sum_{i=1}^{n} \sum_{k=1}^{K} p(k \mid \mathbf{y}_i) \log(p(k \mid \mathbf{y}_i)) / n \tag{8}$$

where: E^* denotes an expectation estimator and H_K is the measure we are interested in.

We proceed fitting K_{max} models with different order (K = 1, 2, ..., K_{max}) and we evaluate the expected entropy (8) for each of them. The model which results in a minimum of this measure will be considered the optimum model. The complete algorithm of the *learning* phase can be summarized as follows:

EM-Algorithm with Model Order Estimation

1. K = 0, H_{opt} = 0, K_{opt} = 1.
2. K = K+1.
3. Fit the K-order model to data using the EM-Algorithm (eqs. 2-6).
4. Calculate expected value of H_K (Equation (8)).
5. If $H_K < H_{opt}$ then Hopt = H_K ; K_{opt} = K; and $\boldsymbol{\Psi} = \boldsymbol{\Psi}_{opt}$.
6. If K < K_{max}, then repeat (2).
7. Update actual model order K with optimal model order: K = K_{opt}.
8. Update actual model parameters $\boldsymbol{\Psi}$ with optimal model parameters $\boldsymbol{\Psi}_{opt}$.

B. Anomaly Detection

During detection, the behavior model has been already fitted and is available for making inferences about a new data presented to the system. Our objective is to define some penalty λ, which varies from 0 (zero) to 1 (one) (e.g. $0 \leq \lambda \leq 1$), indicating the degree of normality concerning this realization from certainly abnormal (λ = 0) to a certainly normal (λ = 1) behavior.

[3] This should be easily verified by simple inspection of entropy expression. A formal treatment can be found in [5].

We have defined a detection procedure formed by two basic steps: a (Bayesian) classification inference and a cluster pertinence inference.

The classification inference is straightforward for parametrical mixture models and consists of evaluation of the posterior cluster probabilities conditioned to new data **y'**, p(k | **y'**), for k = (1, 2,..., K).

Cluster pertinence inference is a little more complex. The considered approach consists in evaluating the probability of new data being contained in some pertinence interval (Π_k), defined as a function of cluster distribution parameters (μk and $\mathbf{R}$ k, for example) and the observation y', which should be formally expressed as following (Equation (9)):

$$p(\mathbf{y}' \in \Pi_k \mid k) = \int_{\Pi_k} g_k(\mathbf{y}, \boldsymbol{\theta}_k) d\Pi_k \tag{9}$$

Such probability should, indeed, look like some kind of cumulative distribution function (cdf), if we define Π_k as stated in Equation (10), below[4]:

$$\Pi_k = \left\{ \mathbf{y} \in \Re^d \mid \frac{\left\| (\mathbf{y} - \boldsymbol{\mu}_k) \right\|^2}{\left\| \mathbf{R}_k \right\|} \geq \gamma^2 \right\} \tag{10}$$

where: $\| \ \|^2$ and $\| \ \|$ denote some type of norm operators, and γ is a constant that should depend on **y'**.

Finally, detection penalty should be defined as (Equation (11)):

$$\lambda(\mathbf{y}') = \sum_{k=1}^{K} p(k \mid \mathbf{y}') p(\mathbf{y}' \in \Pi_k \mid k) \tag{11}$$

4 Manet Traffic Characterization and Behavior Model Construction

The goal here is to construct a model of behavior to characterize the normal traffic conditions in a Manet. Knowing there isn't a common place about which traffic pattern would be typical in a Manet, the characterization of what would be a normal traffic should be done for each case.

Also, it may be difficult to obtain real samples of Manet traffic in operation which are free of possible intrusion vestiges. An alternative is the execution of simulations.

[4] This is a good choice for symmetrical kernel distributions, as the Gaussian distribution used in our experiments. Asymmetrical distributions should have different definitions.

Thus, the pretension here is to validate a behavior intrusion detection process using simulated data.

In order to create our normal traffic profile for simulation, we use the following assumptions:

- Control traffic: basically consisted of the traffic generated by the routing protocol (UDP) and ARP (neither UDP nor TCP).
- Applications: four kinds of traffic generated by different applications in all of the network nodes are considered. Their parameters are adjusted to produce an average occupation of the wireless links of around 20% of total capacity.
- The simple remote session (telnet) uses TCP; the generated traffic is bidirectional; the interval between messages is defined by a Poisson process; and multiple sessions are opened between different origins/destinations, being the origin and destination nodes (uniformly distributed), the starting time (Poisson process) and the session burst (normally distributed) randomly defined.
- The blast data transfer (FTP) uses TCP; the "file" size is random (normally distributed); and multiple transfers between different origins/destinations are done, being the origin and destination nodes (uniformly distributed) and the starting time (Poisson process) randomly defined.
- The constant bit rate (CBR) data transfer (videoconference) uses UDP; the CBR rate is fixed at 128 kbps; there are multiple transfers between different origins/destinations, being the origin and destination nodes (uniformly distributed), the starting time (Poisson process) and the session duration (normally distributed) randomly defined.
- The simple application of asynchronous question-answer (ping) uses ICMP; it always send 4 requisitions, separated in time by 1 second; an answer is always sent; and multiple transfers between different origins/destinations are done, being the origin and destination nodes (uniformly distributed) and the starting time (Poisson process) randomly defined.
- Mobility model: the random waypoint algorithm model developed by CMU is adopted[5]. A Manet of 50 nodes in a 250m x 250m area and a transmission range of 50m is used, for simulation purposes, resulting in an average neighborhood of 6.28 nodes.
- The simulation time for model construction is 1000 seconds.

Our objective is to fit a Gaussian mix model to the traffic generated in accordance with the premises defined above, in order to detect traffic anomalies caused by DoS and scan attacks. A crucial issue here is the definition of which variables reflecting the Manet traffic conditions should be modeled (normal behavior characterization) and monitored (detection).

Behavior models are created separately for TCP, UDP, ICMP and IP traffic. As Table 1 shows, for each model a group of pertinent variables is monitored. Table 1 also shows which type of attacks is intended to be detected using a GMM normal behavior model and having as reference data the simulated traffic, generated according to the premises stated above.

[5] http://www.monarch.cs.cmu.edu/cmu-ns.html

Table 1. Monitored Variables. Types of attacks that are intended to be detected using GMM normal behavior model.

Monitored Variables		
Behavior Model	**Variables to be monitored**	**Possible detected attacks**
TCP	-number/rate of connections or incomings -each connection duration -tcpInErrs[6] -tcpNoPorts[6]	-TFN and TFN2K -stacheldraht -shaft -mstream -TCP scanner
UDP	-udpInDatagrams -udpInErrs[6] -udpNoPorts[6]	-trinoo -TFN and TFN2K -stacheldraht -shaft -UDP scanner
ICMP	-icmpInEchos -icmpOutEchos -icmpInErrs[6]	-smurf -TFN (ping flood) -stacheldraht -shaft
IP	-ipReasmFails[6]	-TFN2K (Traga3)

5 Implementation and Experimental Results

The figure 1 illustrates the simulation data processing to verify the applicability of the behavior intrusion detection techniques to Manet networks. *trafficgen* is a script that is used to generate the *ns-2* input files, allowing for adjustments in the simulation model (e.g. 50 nodes Manet, 250m x 250m area, transmission range of 50m etc.). The *ns-2* package is used for the simulation and generates a trace file containing all the generated packages, forwarded and received in all of the net nodes (*trafego.out*). However, all the MIB variables must be saved and monitored in each node. Therefore, this file is decomposed in several other files, one for each node of the net, by the *ns2tcpdump* program. Inside each file generated by *ns2tcpdump* only the packages

[6] These variables are observed with zero mean and variance in construction data of the reference model, as there is no error conditions in normal traffic generated by simulation. The use of these variables generates singularities in the maximization function of the EM algorithm and, therefore, they are avoided in the results presented in this paper. In real networks, however, these variables present not null values, reflecting the occasional faults of the monitored system/network.

generated, received or forwarded by the same node are actually written. These files are equivalent to a package dump file captured by a net analyzer with capture interface set to non promiscuous mode. These files also transforms the packages traces generated by *ns-2* in packages that look like those captured by a net analyzer: all the fields of the layers 3 and 4 are fulfilled (including IPv4 with 4 bytes) and an absolute timestamp, compatible with the relative time measure used by *ns-2*, is inserted into each package. The results from *ns2tcpdump* are files **.pcap*, which have the format compatible with raw package dump of the *libpcap* library. Once this format is largely supported by several net analyzers, for instance, ethereal, the files *.pcap can be visualized and analyzed by this tools. After that, each one of this files is processed by the *tcpdump2mib* that produces as output (**.mib* files) a list of samples of the MIB variables values sampled in a time interval that can be defined by parameter passing at the command call.

We assume that each Manet node executes one local instance of the IDS, called L-IDS. The L-IDS data collector executes periodic pooling to a local SNMP agent [6]. This is equivalent to processing the IDS algorithms with the values assumed by the MIB variables that are stored inside the *.mib files. It is important to notice that the sampling period passed to the program *tcpdump2mib* (i.e. for the *.mib file generation) does not have to be the same period of pooling used by the L-IDS extractor module. Actually, the pooling period is a lot bigger than the period used by *tcpdump2mib*.

To make the training and the model adjustment, the training events (variable samples) generated in all network nodes are processed in a single L-IDS, providing an GMM adjustment to the reference data (events) that is independent of the Manet node. The result of this stage is distributed to all L-IDSs in the network.

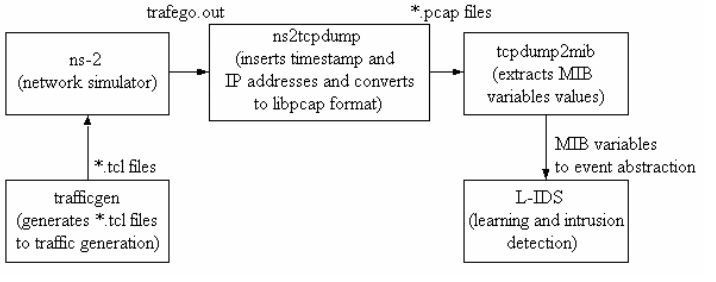


Fig. 1. Simulation process

Two traffic models have been closely analyzed: TCP and UDP. Using these models separately creates an implicit discrimination between all the UDP and TCP generated traffic. Thus, the behavior model using UDP will be useful to model only the videoconference application and the routing protocol. On the other hand, for TCP, the traffic generated by Telnet and FTP applications is modeled.

In case of UDP model, only the udpInDatagrams (UDP datagrams that go into a node) and ipForwDatagrams (IP datagrams forwarded by the node) variables are used. Once this variables are monotonically growing, the observation (updIn; ipForw) is

defined as the learning event generation (realization), which value is obtained subtracting from the present value of "udpInDatagrams; ipForwDatagrams" (current periodic pooling) its predecessor value (previous periodic pooling). The pooling period was adjusted to the same interval of the OLSR TC (equal to three times the HELLO interval, e.g. 6s).

Concerning GMM model for the UDP traffic model, adjusted to the simulation data, the formation of two well defined clusters was observed: the first one, with average of (6,3; 93,9) datagrams and standard deviation of (2,2; 39,7) datagrams. Certainly, this cluster indicates traffic conditions of a node that is not receiving or forwarding any package from the videoconference application. Another cluster, with average of (203; 101) datagrams and with standard deviation of (21,1; 47,1) datagrams resulted from the videoconference traffic (source CBR 128kbps) modeling. Obviously, there is a contribution of the OLSR protocol traffic over the average and the standard deviation of this cluster values. The correlation between the variables are positive, but small (36,7 datagrams).

For the generation of the DoS attack, it is simulated the generation of an UDP CBR (2Mbps) traffic in four randomly chosen origin nodes in direction to an unique destination node. Applying the detention model, anomalous situations are detected in all the nodes that forward the traffic from the origin to the destination. This result is interesting from the point of view of DDoS detention. The detection was only possible thanks to the combined analysis of two variables udpInDatagrams and ipForwDatagrams.

We are also interested in evaluating the response measures that could possibly be activated by the L-IDS in the nodes detecting the attack, in order to mitigate the attack effects. Obviously, the node that receives all generated traffic (from all its neighbors) will quickly become unavailable (the *ns-2* accuses the generation of some forward errors and the disposal of the destined node neighborhood packages). However, although the far nodes are generating/forwarding a non-expressive amount of data, they are not necessarily broken by the attack. As the intrusion detection system identifies anomalies in all nodes in the forward path, these nodes could possible interact to block the forwarding of packages that come from the compromised origin. This forwarding must be blocked based on the enlace address and not based on the IP datagram destination addresses, because these ones are easily faked and, in more advanced DDoS attacks, they are constantly modified (to each package).

In the case TCP model, tcpPassiveOpens (number of open passively connections in the node) and tcpInSegs (number of received segments, including the ones with error and for connection opening) are used as MIB variables. Similarly to the UDP case, a pooling period equal to the OLSR TC interval is defined (e.g. 6s). The observations (tcpPO ; tcpIN) are obtained as the difference between the value of (tcpPassiveOpens; tcpInSegs) in the current and preceding consultation. To avoid singularities (i.e. a formation of a cluster with average zero and small variance for tcpPassiveOpens), the events in which tcpPassiveOpens was equal to zero are discarded as normal in the learning and in the intrusion detection processes. Concerning to the adjustment, in this case, it is observed the formation of two clusters with averages at (1,11; 38,41) and at (1,05; 97,11), shaping respectively the telnet and the ftp.

For the generation of a scanner attack, an origin-destine pair is randomly chosen and this origin sends TCP connection solicitations to the destination, in a rate of 10 solicitations per second. In destination, a drain is made in which, to each 30 connection

solicitations, one is accepted (i.e. indicating one "match" with one service that is answering). As long as the values of the MIB variables start to reflect this additional traffic, the attack is detected by the destination node, with a null false negative rate.

6 Conclusions and Future Work

We have presented a new anomaly IDS design for statistic behavior modeling of a network. It uses a parametric Gaussian mixture model for behavior modeling with a Bayesian classification intrusion-detection. This model aims to permit the simultaneous modeling of different types of events (e.g. applications) that have influence on the set of variables available for monitoring. The preliminary experimental results indicate that this kind of model can be adjusted with a carefully choice of variables to be modeled and monitored. Due to the large cost of monitoring packets in a Manet, we have chosen to use MIB variables. These variables are easily provided by SNMP agents. However, the proposed intrusion detection model by behavior anomaly is still in its first stages of development and it has just been used with synthetic data that do not represent necessarily the real behavior of a network. Due to this fact, beyond the need of a further validation with real data, the model presents some important limitations that must be investigated and become more flexible. Moreover, the parametric Gaussian mixture model is not suitable for modeling complex data that do not have normal features.

Finally, as future work, we suggest the validation of this model with experiments that use real data. Furthermore, a lot of improvements of model conception preconditions can be done, like the use of other types of kernel functions, the use of semi-parametric mixture models [14], the adoption of stochastic models (e.g. Markov process) for eliminating the statistic independence pre-condition between the events, among others.

References

1. Hao Yang, Haiyun Luo, Fan Y, Songwu Lu, Lixia Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications - February 2004 – pp 2-11, 2004.
2. R. Puttini; R. de Sousa.; L. Me – Preventive and Corrective Protection for Mobile Ad Hoc Network Routing Protocols. In Proceedings of 1st International Conference on Wireless On-demand Network Systems in Lecture Notes on Computer Science, Springer, 2004.
3. R. Puttini; Z. Marrakchi and L. Mé - Bayesian Classification Model for Real-Time Intrusion Detection, 22th International Workshop on Bayesian Inference and Maximum Entropy Methods in Science and Engineering (MAXENT'2002). August 2002.
4. Y. Zhang and W. Lee – Intrusion detection in wireless ad hoc networks. Proceedings of 6th ACM Annual International Conference on Mobile Computing and Networking (MOBICOM 2000), ACM Press, New York, pp. 275-283, 2000.
5. V. Mittal and G. Vigna. Sensor-based intrusion detection for intra-domain distance-vector routing. In R. Sandhu, editor, Proceedings of the ACM Conference on Computer and Communication Security (CCS'02), Washington, DC, November 2002. ACM Press.

6. R. Puttini; J.M. Percher; L. Me; R. de Sousa - A Fully Distributed IDS for Manet. In Proceedings of 9th IEEE International Symposium on Computers Communications, 2004.
7. G. Vigna, S. Gwalani, K. Srinivasan, E. Royer, R. Kemmerer – A Intrusion detection tool for AODV-based ad hoc wireless network. In Proc. 20th Annual Computer Security Applications Conference (ACSAC2004), 2004.
8. H. Yang, X. Meng and S. Lu, "Self-Organized Network Layer Security in Mobile Ad Hoc Networks", in the Proceedings of ACM Workshop on Wireless Security – 2002 (WiSe'2002), in conjunction with the ACM MOBICOM2002, September, 2002.
9. Y. Huang, W. Fan, W. Lee, and P. Yu. Cross-feature analysis for detecting ad-hoc routing anomalies. In The 23rd International Conference on Distributed Computing Systems, May 2003.
10. C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based intrusion detection system for AODV. In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03), October 2003.
11. S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehaviour in mobile ad hoc networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, August 2000.
12. G. J. McLachlan, D. Peel, K. E. Basford and P. Adams, "The EMMIX Software for the Fitting of Mixtures of Normal and t –Components", Journal of Statistical Software, v. 04, 1999.
13. Dempster, A. P., Laird, N. M., and Rubin, D. B., Journal of the Royal Statistical Society B 39 ,1-38 (1977).
14. Roberts, S. J., Everson, R., and Rezek, I., Pattern Recognition, 33:5, pp. 833-839 (1999).
15. Johnson, R. A., Wichern, D. A., Wichern, D. W. , "Applied Multivariate Statistical Analysis – 4th Edition", Prentice-Hall, 1998.

Locally-Constructed Trees for Adhoc Routing

Ricardo Marcelín-Jiménez*

Electrical Eng. Dept., UAMI;
Atlixco 186; 09340 México D.F., México
calu@xanum.uam.mx

Abstract. We present a family of self-stabilizing distributed algorithms to built a spanning tree on the underlaying communications graph of an adhoc wireless network. Next, based on this principle, we show how to construct two overlaying trees which are suitable for routing tasks.

1 Introduction

Routing using local information has been considered an alternative approach to cope with the main drawbacks of traditional strategies, such as scalability or fault-tolerance [1], [2], [4], [5], [8], [11]. Most of the routing algorithms using local position information, perform a preliminar process on the underlying graph, in order to produce a planar one where working requirements are met [7], [9].

We present a routing algorithm for adhoc wireless nets where each node knows its coordinates on the plane, and the relative coordinates of its neighbors in order to built up two overlaying spanning trees where routing operations have place. Each tree is a self-reconfigurable structure which is able to tolerate links and node failures.

The rest of this work includes the following parts: section 2 presents the theoretical framework that supports our proposal, section 3 introduces our general distributed spanning tree algorithm and shows how routing tasks can be implemented on top of two overlaying structures of this kind, section 4 offers some performance metrics about 4 different types of construction algorithms, based on the principles developed in section 3, finally section 5 is a discussion about the applications and directions for further work.

2 Assumptions and Models

This work deals with distributed algorithms in an *asynchronous* network model. The asynchronous network is a point-to-point (store-and-forward) communication network, described by a *communication graph* $G = (V, E)$, of order $|V|$ and size $|E|$, where the set of nodes V represents a set of state machines called the processors of the network and the set of links E represents communication channels operating between them. Let x and y be two nodes in V. There is a link from

* Visiting the CINVESTAV under contract Marina-CONACyT 2002C013199A.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 194–204, 2006.

x to y if and only if x can talk directly to y. In our simplified model, we ignore all radio propagation effects and make all nodes have the same transmision range which we set to be equal to 1. The graph G is called the *unit distance graph*: there is a link between any two nodes whose distance is less than or equal to 1. The assumptions we make are that: a given MAC protocol is already in operation on the underlying network, all nodes know their geographic location, each node knows its immediate one-hop neighbors (those within its radio range) and, finally, we assume that all nodes but one, have a west-ward (north-ward) neighbor. Any node may suffer a crash failure and will be considered permanently out of service from then on.

We usually denote the ith processor in the system by p_i. FIFO queues are used to model asynchronous delivery of messages. A communication link is either unidirectional or bidirectional. A unidirectional communication link from process p_i to p_j transfers messages from p_i to p_j. The abstraction for such a unidirectional link is a first-in-first-out queue q_{ij}, that contains all messages sent by p_i to its neighbor p_j, that have not yet been received. The bidirectional communication link between p_i and p_j is modeled by two FIFO queues, one from p_i to p_j and other from p_j to p_i.

A *system configuration* c is a full description of a distributed system, at a particular time and consists of the state of every processor and the content of every queue. We use the term *step* for a computation step and we denote it by a. Let c_1 and c_2 be two configurations of the system, where c_2 is reached from c_1 by a single step a of a processor; we denote this fact by $c_1 \xrightarrow{a} c_2$, also we say that a is *applicable* to c_1. An *execution* $(c_1, a_1, c_2, a_2, \ldots)$ is an alternating sequence of configurations and steps such that $c_{i-1} \xrightarrow{a_{i-1}} c_i$.

No common memory is shared by the node's processors, and each node p_i has a distinct *identity* i. Each node processes messages received from its neighbors, performs local computations, and sends messages to its neighbors. All these actions are assumed to be performed in negligible time. All of the messages have a fixed length and may carry only a bounded amount of information. Each message sent by a node to its neighbors arrives within some finite but unpredictable time, unless a message lost happens. To model such events we extend the definition of a step to include environment steps of type $\text{loss}_{ij}(m)$ that is applicable to a configuration c_k in wich q_{ij} contains the message m. This step results in a configuration c_{k+1} in which m is removed from q_{ij}.

A *fair* execution is an execution in which, if infinitely often a processor has a step to execute then the processor executes this step infinitely often. Also, we do require that if a message is sent infinitely often, the message is received infinitely often. To satisfy fairness the receive step must be executed infinitely often while the loss step should not be executed infinitely often.

A *self-stabilizing* system can be started in an arbitrary configuration and will eventually exhibit a desired "legal", behavior. We define this legal behavior by a set of legal executions denoted LE. Every system execution of a self-stabilizing system should have a suffix that appears in LE. A configuration c is *safe* with regard to a task LE and an algorithm if every fair execution of the algorithm

that starts from c belongs to LE. An algorithm is self-stabilizing for a task LE if every fair execution of the algorithm reaches a safe configuration with relation to LE [3].

The following complexity measures are used to evaluate performance of distributed algorithms operating on the above network. The *communication complexity* is the total number of messages sent during execution of the algorithm. The *time complexity* is the maximum time passed from its start to its termination, assuming that the time of delivering a message over each link is at most one unit of time. This bounded delay is assumed only for evaluating time complexity.

3 The Algorithm

This section is intended to sketch, from a formal view, the correctness of our setup and routing algorithms. It also fixes some bounds on the complexity of the whole process.

We claim that, once the process attains a steady condition, a distributed spanning tree is built on the set of participating nodes. The *ancestor*, *descendant*, and *level* concepts furtherly required are defined recursively: the root is axiomatically considered to be its own father, with its level equal to 0. A node's ancestor is said to be its father or any ancestor of its father. A node's level is said to be 1 plus the level of its father. A node's descendant is its sibling or a sibling of any descendant.

A START message indicates that the node must (re)trigger its father-searching procedure. During operations, nodes exchange three different messages: HELLO, DESCENDANTS and ANCESTORS. The HELLO message is issued by a node that has selected a place from its westward neighbors to be its father on the structure under construction. The receiver considers the sender to be its direct sibling, and gets prepared for further information coming from this place. The DESCENDANTS message is issued by a node to inform its father about the list, called Upper, of siblings (either direct or not) that can be reached through it. Finally, the ANCESTORS message is issued by a father to let its direct siblings know the list of nodes, called Lower, on the path from the resulting root to it.

We said that this algorithm evolves in cycles, each of them having two phases: during the first one, the convergecast, information flows from the leaves to the root, by means of the HELLO and DESCENDANTS messages. In the second phase, the broadcast, information goes from the root to the leaves, by means of the ANCESTORS messages. Each node has two timers that alternatively work to mark the ending of the corresponding phase. Upon the expiration of a timer the node is compelled to finish the proper flow with the information so far collected (See fig. 1).

Lemma 1. *There is exactly one node s, that becomes the root.*

Proof. Node s exists since there is, at least, one west-most node. i) if there is exactly one such place, then node s does not have any neighbor j, with relative polar coordinates (r_{js}, θ_{js}), for any $r_{js} > 0$ and $\theta_{js} \in (\frac{\pi}{2}, \frac{3\pi}{2}]$. Then, according

```
< 1> upon the reception of START
< 2>      select j ∈ Neighbors_i, such that
< 3>      j lies on the plane centered in i
< 4>      and has relative position (r_ji, θ_ji),
< 5>      r_ji > 0 and θ_ji ∈ (π/2, 3π/2];
< 6>      if does not exist such j
< 7>      then i am the root;
< 8>      else father = j;
< 9>           send HELLO to father
<10>           start timer_1

<11> upon the reception of HELLO from j
<12>      Sons_i = Sons_i ∪ {j};
<13>      ack_j = F;

<14> upon the expiration of timer_1
<15>      for each k ∈ Sons_i : ack_k == F
<16>           Sons_i = Sons_i \ {k};
<17>           Upper_i = Upper_i \ Upper_k;
<18>           cancel ack_k;
<19>      if i am the root
<20>      then Lower_i = Lower_i ∪ {i};
<21>           for any k ∈ Sons_i
<22>                send ANCESTORS with Lower_i to k;
<23>      else Upper_i = Upper_i ∪ {i};
<24>           send DESCENDANTS with Upper_i to father;
<25>           start timer_2
<26>           for any k ∈ Sons_i
<27>                ack_j = F

<28> upon the expiration of timer_2
<29>      Lower_i = {i};
<30>      for any k ∈ Sons_i
<31>           send ANCESTORS with Lower_i to k;
<32>           ack_j = F
<33>      goto <2>;

<34> upon the reception of DESCENDANTS from j
<35>      if j ∈ Sons_i
<36>      then Upper_i = Upper_i ∪ Upper_j;
<37>           ack_j = T;
<38>           if ¬∃k ∈ Sons_i : ack_k == F
<39>           then stop timer_1;
<40>                goto <19>;

<41> upon the reception of ANCESTORS from j
<42>      if j == father and timer_1 is off
<43>      then stop timer_2;
<44>           start timer_1;
<45>           Lower_i = Lower_j;
<46>           goto <20>;
```

Fig. 1. Construction algorithm in node i

to the construction rule, it becomes the root. ii) assume there is more than one node having the same west-most (horizontal) coordinate, then all of them but the south-most will have at least one neighbor with relative polar coordinates within the selection range. Therefore, the south-most is the only place with conditions to become the root (see lines $< 1 > \ldots < 10 >$ of fig. 1).

Lemma 2. *There exists one single path from any node to the root.*

Proof. We proof by induction on the levels of the resulting structure. As usual, the root has level 0 and knows exactly one way to itself. Assume that our statement is true for all nodes up to level $n > 0$, therefore any node of level $n + 1$ only knows one way to the root that passes through its single ancestor of level n, i.e. its father.

Lemma 3. *Upon the termination of the first cycle, a distributed spanning tree is built on the set of active nodes and each one knows the list of lower and upper places that are reachable through its father and siblings, respectively.*

Proof. With the exception of the root, each node selects exactly one link (going to its father). Therefore, we have $|V| - 1$ links that make up the resulting structure.

We state that for any node j, if every $k \in \text{Lower}_j$ is active, then $s \in \text{Lower}_j$ and $j \in \text{Upper}_s$, as consequences of the converge and broadcast phases, respectively. Suppose this condition is true for any two nodes i and i' of level n and m, respectively. Also, suppose that i needs to reach i'. If $m < n$, then either $i' \in \text{Lower}_i$ or there exists exactly one path from i to i' that passes through the root s. On the other hand, if $m \geq n$ then, unless $i' \in \text{Upper}_i$, it is also granted that there exists exactly one path from i to j that passes through the root s.

We have shown that it is possible to find exactly one path between any two nodes, and also that the resulting graph has a minimum number of links (see lines $< 11 > \ldots < 13 >$ and $< 34 > \ldots < 46 >$ of fig. 1).

Lemma 4. *A node that loses the link to its father, eventually selects a new one and resynchronizes its subtree cycle with the rest of the structure.*

Proof. Suppose a node i has a direct sibling j, which in turn has a direct sibling k. Upon the event of a failure in j, two links will be dismissed: (i, j) and (j, k). Nevertheless, only k will be in charge of the recovery procedure, selecting a new father to reconnect its subtree. Recovery starts when k sends a HELLO message to its new father. This means that the timer 2 of the issuing node k has elapsed and it takes for granted that its former father is lost. Therefore, k starts its convergecast phase. In due time, it gathers all of the information about the upper nodes it is able to reach and now sends a DESCENDANTS message to its new father j'. Now k starts timer 2 again and sits down waiting for an ANCESTORS message coming from j'. At the other end of the new link, j' may be either in the convergecast or in the broadcast phase. In the first case, j' was just waiting for the DESCENDANTS message to update its $\text{Upper}_{j'}$ list. In due time, it will send an ANCESTORS message back to k wich will help it to update

its Lower_k list. In the second case, j' sends an ANCESTORS message back to k as in the previous case, but j' will not be able to update its own information up to the next cycle (see lines $< 28 > \ldots < 33 >$ of fig. 1).

We claim that the task ST of legitimate sequences is defined as the set of all configurations in which every configuration encodes a spanning tree of G. The preceeding lemma grants that it takes 2 cycles, at most, in order to reach a safe configuration that codifies a new tree.

Lemma 5. *A node with a timer that prematurely expires eventually updates with the correct structural information and resynchronizes its subtree cycle with the rest of the structure.*

Proof. Suppose timer 1 ends at node i and later a DESCENDANTS message is received at i from a direct sibling j. In this case, j has already been dismissed and the message is not accepted. Eventually, j will not receive the corresponding ANCESTORS message and will take for granted that its father is lost. This will trigger its recovery procedure as in the preceeding lemma(see lines $< 14 > \ldots < 27 >$ of fig. 1).

Suppose timer 2 ends at node i and later an ANCESTORS message is received a i from its father. In this case, as soon as timer 2 finishes, i starts its recovery procedure and selects a new father, therefore in the case of a late message from the former father, it will not be accepted(see lines $< 28 > \ldots < 33 >$ of fig. 1).

Lemma 6. *A cycle has message complexity $O(|V|)$ and time complexity $O(|V|)$, while a recovery takes an overhead $O(1)$.*

Proof. During the first cycle, a HELLO message is sent over each of the links that will make up the resulting tree. Next, at the end of the convergecast, a DESCENDANTS message will climb the same links to the root. Finally, during broadcast, an ANCESTORS message will flow down the leaves exactly on the same links but in opposite direction. From then on, only DESCENDANTS and ANCESTORS will traverse the resulting structure, unless an active node starts the recovery procedure sending, for one single time, a HELLO message to its new father. The rest of the synchronization can be regarded as being part of an ordinary cycle (see lines $< 1 > \ldots < 10 >$ of fig. 1).

So far, it has been shown that is possible to built up a spanning tree that keeps updated its structure information despite of link or node failures. Our construction is based on the local knowledge each node has about the position of its neighbors. Each node, except the resulting root, selects a neighbor within a geometric range. Clearly, this range can be reoriented, i.e. we can construct an north-ward tree, instead of a west-ward. But, what if we construct both trees at the same time? We will have two overlaying, self-reconfigurable, structures to profit from, as in a railroad system. It may have a great impact on routing procedures. Suppose we have an east-west tree T_{EW}, and a south-north tree T_{SN} on the same underlaying network. If node i requires to reach node i', it is granted that there are at two routes, one on each tree, and it is possible to

install a performance metric to choose the best one. But also, in case of local problems, it could be possible to take an alternative path around the affected area. We present a very simple routing algorithm based on this possibility.

Let us assume again, that node i has an application message m, for node $d = i'$, then it encapsulates both data inside a routing packet that we will call INFO. Each place on the way from source to destination will obey the following procedure (See fig. 2).

```
< 1> upon the reception of INFO, carrying m to d
< 2>      for some T and T', either T_NS or T_EW
< 3>      if i == d
< 4>      then receive m;
< 5>      else
< 6>      if ∃k ∈ Sons_i^T, d ∈ Upper_k^T
< 7>      then forward INFO to k;
< 8>      else
< 9>      if d ∈ Lower_i^T
<10>      then forward INFO to father of T;
<11>      else
<12>           let T' be the tree with the nearest root
<13>           if i is not the root of T' and father is up
<14>           then forward INFO to father of T';
<15>           else stand by until recovery;
```

Fig. 2. Routing algorithm in node i

Lemma 7. *Unless d crashes, m eventually arrives to d.*

Proof. It is a structural property of the overlaying trees (lemma 3). In this case each node must look at the two trees it belongs to, in order to find a direct route to d, or forwarding m to the closest root r' (either of T_{EW} or T_{SN}) where it is granted to exist a direct branch from r' to d (Nevertheless, it can find a better route on its way to r'). Finally, if m arrives to r' and there is not a built up branch going to d, it means that there has been a failure and it is better to wait until recovery is finished. Once the system is recovered, r' will forward m towards d, unless d is lost.

We leave for the next section some experimental evidence about the diameters of the resulting trees, which bound the complexity of the routing procedure.

4 Experimental Results

For each graph here considered we run 4 different families of algorithms, defined according to their tree construction procedures. Each family is said to perform an east-west scanning which produces a so-called horizontal (H) tree, next a similar procedure is performed according to a south-north scanning which produces a vertical (V) tree.

Basically all of the construction rules can be explained under the same principle, for an east-west (south-north respectively) scanning, take any node on a graph and select all of its incident edges going to the west (respectively north) and dismiss them all but one. Differences arise from the way this surviving edge is chosen:

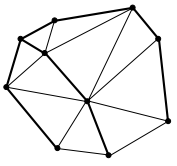


Fig. 3. H tree produced with A1

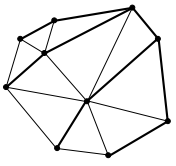


Fig. 4. V tree produced with A1

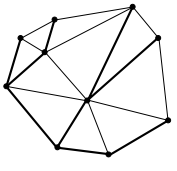


Fig. 5. H tree produced with A2

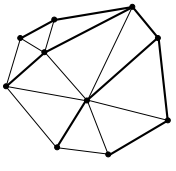


Fig. 6. V tree produced with A2

algorithm 1 (A1) for each node, we consider the west-ward neighbors' edges and dismiss all but the first edge in counterclockwise sense (fig. 3). Next we perform the same operation over the 90 degrees rotated graph or, equivalently, from each node considering its north-ward neighbors' edges(fig. 4).

algorithm 2 (A2) for each node, select all of its incident edges going to the west and dismiss them all but the first on a clockwise sense (fig. 5). In contrast, for a vertical scanning, select all of the incident edges going to the north and dismiss them all but the first on a counterclockwise sense (fig. 6).

algorithm 3 (A3) again, in the horizontal scanning, select all of the incident edges going to the west and dismiss them all but one which is randomly picked up(fig. 7). In contrast, for a vertical scanning, select all the incident edges going to the north and dismiss them all but one which, as could be expected, is also randomly picked up(fig. 8).

algorithm 4 (A4) for each node, consider all of its incident edges going to the west and dismiss them all but the one closest to the horizontal axis. Next, we perform the same operation over the 90 degrees rotated graph or, equivalently, we dismiss all of the edges going to the north but the one closest to the vertical axis(fig. 10).

Three measures will be considered as a common basis in order to evaluate and compare the algorithms under study: i) HV correlation measures the number of edges belonging to the horizontal tree that also appear in the second one

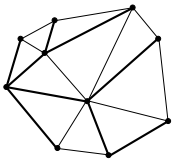


Fig. 7. H tree produced with A3

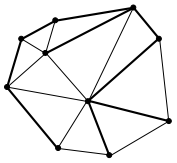


Fig. 8. V tree produced with A3

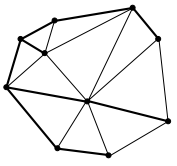


Fig. 9. H tree produced with A4

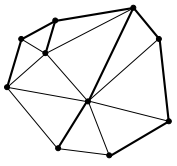


Fig. 10. V tree produced with A4

(vertical), ii) the mean diameter measures the mean longest path on the resulting trees, iii) finally, the degree and max. degree frequencies show the statistics of the nodes on the resulting constructions.

Table 1. 95% confidence intervals for the average correlation between H and V trees

	HV %correlation
A1	15.6 ± 0.2
A2	41.4 ± 0.2
A3	43.4 ± 0.3
A4	6.5 ± 0.1

Table 1 presents the HV correlation measured on each couple of trees constructed according to the 4 algorithms which were ran on 100-nodes graphs. Notice that in algorithm 1, the surviving edge is the last-one in clockwise sense, either on EW or SN scanning. In algorithm 2, the surviving edge is the first-one in clockwise (counterclockwise) sense for EW (SN) scanning. The poor performance on the HV correlation between the resulting trees is due to this selection rule, for it happens frequently that SN-surviving edge of one node is the same EW-surviving edge of a second node. In algorithm 3, the surviving edge is randomly selected in both scanningsm which does not seem to be a good rule, at least for the HV measure. In algorithm 4, the surviving edge is the one closest to the horizontal (vertical) axis for an east-west (south-north) scanning. This selection produces the best (lowest) correlation in all of the cases.

Table 2 shows how the mean diameter evolves according to the graph order. The most interesting result is the way diameter grows in algorithm 3, which is completely different from the rest of the algorithms that have a smooth growing rate that follows an empirical law of the form $cn^{1/3}\log(n)$.

Table 2. 95% confidence intervals for mean diameters

order	20	40	60	80	100
A1	9.2 ± 0.06	14 ± 0.09	18 ± 0.11	21 ± 0.09	23 ± 0.16
A2	9.1 ± 0.07	14 ± 0.05	18 ± 0.20	21 ± 0.20	23 ± 0.29
A3	11 ± 0.07	17 ± 0.08	21 ± 0.15	21 ± 0.59	13 ± 0.92
A4	9.1 ± 0.07	14 ± 0.08	18 ± 0.10	21 ± 0.13	22 ± 0.42

Table 3. Algorithms A1 to A4, degree and max. degree frequencies

	1	2	3	4	5	6	7	8	9
A1 deg. freq.	0.31	0.47	0.17	0.036	0.0097	0.0032	0.00051	0.00013	0
A1 max. deg.	0	0	0	0.14	0.5	0.29	0.051	0.013	0
A2 deg. freq.	0.32	0.45	0.17	0.038	0.012	0.0033	0.00059	0.00012	0
A2 max. deg.	0	0	0	0.071	0.56	0.29	0.059	0.012	0
A3 deg. freq.	0.35	0.4	0.2	0.049	0.0088	0.0013	0.00012	0	0
A3 max. deg.	0	0	0	0.31	0.55	0.13	0.012	0	0
A4 deg. freq.	0.32	0.46	0.17	0.039	0.011	0.0029	0.00073	0.00018	0
A4 max. deg.	0	0	0	0.091	0.55	0.27	0.073	0.018	0

Tables 3 shows the degree distribution for trees built up according to the algorithms under study, all of them ran on 100-nodes graphs. As for degree distribution, all of the tables show similar results which could be considered as a regular feature of the trees obtained according to this scanning principles. As for max. degree distribution, the slight differences arising in algorithm 3 could be the explanation for the results in table 2.

5 Conclusions and Further Work

Position is a source of global knowledge that adhoc wireless networks can profit from. Perhaps it might not be necessary to have a GPS on each node and it will do with two beacons located in orthogonal positions to let each place evaluate its coordinates based on field intensity.

We have introduced different ways to built up two overlaying spanning trees, all of them based on the same principles here presented. The impact of each procedure can be evaluated according to different parameters: mean diameter, mean degree and the number of common links between the resulting trees. We believe that the first two measures indirectly define the complexity of routing, while the last one indicates the robustness of the whole system.

About the experimental work, we should notice that having two trees built up from two different scanning senses makes the overlaying trees look like a subway or train system, this means that most of the nodes might work as an exchange points wich can have a great impact on the routing procedures, i.e. packets

can travel over the horizontal tree and switch their routes to a vertical direction at any node, in order to shorten their path towards a given destination.

All of the procedures under test built up their corresponding trees from the local information that each node has about its neighbourhood. The importance of this approach becomes evident when we consider the following scenario: assume one of the nodes crashes, then only those neighbours directly connected with the missing place will be in charge of the reconfiguration. The rest of the nodes will not be (and do not need to be) aware of the changes triggered by the crash failure.

For further work, it would be interesting to find a tradeoff between timers' length (update rate) and communications overhead. Our solution might be applied in sensor networks too. In such case, this tradeoff would play a key role to lengthen battery lifetime [12],[6]. Also, we believe that the routing procedures here presented can be applied in mobile environments when all the nodes are moving in the same direction. Finally, we think that routing algorithms can be improved as long as we imposse restriction on the structural properties of the resulting trees.

References

1. K. Alzoubi, X.-Y. Li, Y. Wang, P.-J. Wan, O. Frieder, "Geometric Spanners for Wireless Ad Hoc Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 14, No. 5, May 2003.
2. P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia. "Routing with guaranteed delivery in ad hoc wireless networks". In Proc. of Discrete Algorithms and Methods for Mobility (DIALM'99), pages 48–55, 1999.
3. S. Dolev, "Self-Stabilization", The MIT Press 2000.
4. L. Jia, R. Rajaraman, and C. Scheideler "On Local Algorithms for Topology Control and Routing in Ad hoc Networks," Proceedings of the 15th Annual ACM Symposium on Parallel Algorithms and Architectures, pages 220–229, June 2003.
5. E. Kranakis, H. Singh, and J. Urrutia, "Compass Routing on Geometric Networks", In Proceedings of 11th Canadian Conference on Computational Geometry, pp. 51–54, Vancouver, August, 1999.
6. X.-Y. Li, P.-J. Wan, Y. Wang, and O. Frieder, "Sparse power efficient topology for wireless networks, J. Parallel and Distributed Computing, to appear.
7. X.-Y. Li, G. Călinescu, P.-J. Wan, and Y. Wang, "Localized Delaunay Triangulation with Application in Ad Hoc Wireless Networks," IEEE Trans. on Par. Dist. Systems, 2003. To appear. (Modified version of the INFOCOM'2002 paper.)
8. X.-Y. Li, Y. Wang, O. Frieder, "Localized Routing for Wireless Ad Hoc Networks", in proceedings of IEEE ICC, 2003.
9. M. D. Penrose, "On k-Connectivity for a Geometric Random Graph", Random Structures and Algorithms, 15, 145-164, 1999.
10. M. D. Penrose, "The Longest Edge of the Random Minimal Spanning Tree", The Annals of Applied Probability, 7(2) 1997, 340-361.
11. R. Rajaraman, "Topology Control and Routing in Ad hoc Networks: A Survey," SIGACT News, 33:60–73, June 2002.
12. W.-Z. Song, Y. Wang, and X.-Y. Li, "Localized algorithms for energy efficient topology in wireless ad hoc networks," 5th ACM Int. Symp. on Mobile ad hoc Networking and Comp., Tokyo, Japan, 98–108, 2004.

Overlay Small Group Multicast Mechanism for MANET

Uhjin Joung, Hong-Jong Jeong, and Dongkyun Kim*

Department of Computer Engineering,
Kyungpook National University, Daegu, Korea
{ujjoung, hjjeong}@monet.knu.ac.kr, dongkyun@knu.ac.kr

Abstract. In order to provide the multicast service in MANET, a lot of multicast routing protocols have been proposed. Most of them create tree or mesh-based graphs and require network nodes over the tree or mesh to maintain the membership information. In particular, high node mobility causes the tree or mesh to be broken and reconstructed by generating much overhead to manage the membership at network nodes. In accordance with overlay multicast protocols to reduce such overhead, which enables the packet transmission regardless of the movement of intermediate nodes over the paths between group members, we propose an overlay small group multicast mechanism, called SPM (Shortest Path overlay Multicast) for MANET. SPM multicasts packets over the shortest paths from a source to each group member without duplicate packet delivery over common partial paths. When creating a multicast overlay tree, SPM utilizes the route information provided by ad hoc unicast routing protocol without further control messages and any other information. Extensive simulations through NS-2 simulator proved that SPM has better throughput, loss rate and packet transmission delay than MAODV, a typical tree based multicast routing protocol used in MANET.

1 Introduction

MANET is a wireless network where all nomadic nodes are able to communicate each other through the packet forwarding service of intermediate nodes. Specially, since packet forwarding and routing is done via intermediate nodes, the MANET working group in IETF has been trying to standardize its routing protocols [1].

Recently, in order to provide the multicast service in MANET, a lot of multicast protocols have been proposed. However, most of them are based on tree or mesh graphs and they require all network nodes to participate in a multicast routing. In particular, the tree or mesh should be reconstructed when the network topology is affected by the movement of nodes over the tree or mesh. Even more, during the reconstruction with additional control messages, packets cannot be transmitted successfully. In addition, if a forwarding node over the tree or mesh fails to send a multicast packet to its neighbors, other group members reachable via this node cannot receive the packet in the event.

* Corresponding author.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 205–215, 2006.

In order to address these problems, the overlay multicast routing mechanisms which provide multicasting capability using the unicast routing protocol among group members have been proposed [2] [3]. They are not affected by the movement of network nodes if there exist paths among group members because its underlying unicast routing protocol is responsible for route discovery. Since a source should have the information on all group members and put their IP addresses in all transmitted packet headers, they are suitable for the small group multicasting.

Although efficient overlay multicast protocols for MANET have been proposed in [3], they need crucial location information of nodes and there is no mention about how to notify nodes of other nodes' location. In addition, although the paths among group members have the overlapped partial paths, most overlay multicasting techniques require independent unicasting transmissions among group-member pairs to be executed, which results in duplicate packet delivery.

In this paper, we proposed an overlay small group multicast mechanism for MANET, called SPM (Shortest Path overlay Multicast) which delivers packets through the shortest path from a source to each small group member and avoids the packet duplication over common paths. In particular, SPM utilizes route information provided by ad hoc routing protocols without additional control messages for location information and group management. In our previous work [4], we proved that our SPM shows better performance than other overlay multicast protocols for MANET.

The rest of this paper is as follows. In section 2, closely related work to SPM is introduced. In section 3, our SPM protocol is described in detail. We compare SPM with MAODV (Mobile Ad-hoc On-demand Distance Vector) [5], the most well-known multicasting protocol, in section 4. Finally, some concluding remarks are given in section 5.

2 Related Work

2.1 MAODV

Multicasting in MANET has primarily received an attention in terms of providing multicasting capability at network layer. In particular, MAODV [5] allows the route information obtained for multicasting packets to be used in a unicast routing, and vice versa. MAODV builds up a multicast tree based on AODV unicast routing protocol. Each node keeps its Route Table when it requests a route as in AODV. In MAODV, sources, multicast group members and tree members maintain a sharing tree for each multicast group. Each selected group leader periodically broadcasts Group Hello message (GRPH) throughout the whole network, in order to indicate the existence of its group. A joining node participates in the group by especially requesting a route (RREQ), and receiving Route Replies (RREPs) that include the shortest paths to other existing nodes in the multicast tree. The joining node sends ACK message over the best appropriate path (generally, the shortest path) during which all intermediate nodes over the selected path maintain the session information and play roles of

multicast tree members. Figure 1 shows the RREQ/RREP message exchanges in MAODV.

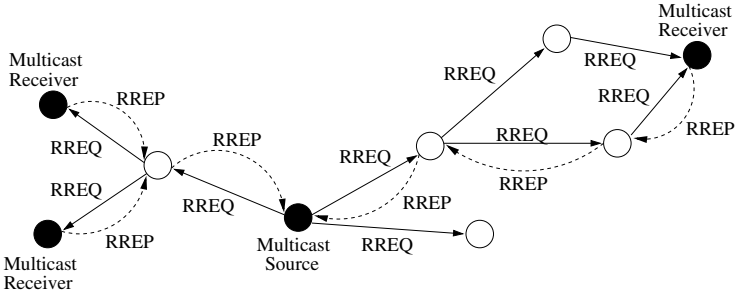


Fig. 1. MAODV Mechanism

However, MAODV has a disadvantage in that the intermediate nodes, even non-group members of a multicast group, need to keep routing table information for a multicast session with much overhead by generating too many control messages in order for each node to maintain it, which results in wasting scarce wireless bandwidth.

2.2 Overlay Multicast

The overlay multicast technique creates a multicast packet delivery tree at application layer and transmits packets by using its underlying unicast routing protocol over the tree. Location-guided multicasting [3], one of the overlay multicast schemes, tries to allow the intermediate nodes to avoid maintaining the global multicast session information. The multicast packets are transmitted from the source to all group members using unicast routing methods through a specific header encapsulation after creating two kinds of tree using the nodal location: location-guided k-ary tree and location-guided Steiner tree. Therefore, it is enough that only the source keeps the group membership information in order to manage the multicast tree. However, the scheme depends on the accurate location of nodes and there is no description on how to notify the nodes of other nodes' location under an environment where node mobility is allowed. Furthermore, all nodes should be equipped with GPS device, which is quite a tough requirement practically. In [4], we compared SPM with the location-guided schemes and proved that our SPM is more suitable for an overlay multicast protocol for MANET.

3 SPM (Shortest Path Overlay Multicast) Mechanism

3.1 Overview of Proposed Approach

We propose SPM (Shortest Path overlay Multicast) to build the multicast packet delivery tree which provides shortest paths from a source to each group member,

which allows the loss rate and packet transmission delay consumption to be minimized. In SPM, the source can manage multicast group membership because it supports a small group. For the membership creation, a node which desires to receive the multicast packets should subscribe to the multicast group by requesting the subscription to the source. Thereafter, the source tries to attach the new member to the existing tree. When a packet is multicasted, the packet header defined in SPM contains the IP addresses of nodes participating in the multicast (the header format is shown in Figure 4) as in other overlay protocols like [2]. In particular, SPM utilizes the routing information provided by its underlying unicast routing mechanism when constructing the multicast packet delivery tree. The route path acquisition techniques are given in detail according to its selected routing protocols in Section 3.4.

Since common paths exist among the shortest paths between the source and each group member, SPM transmits a packet to the last node of the common path in order to avoid duplicate transmissions of the same packet over the path. After arriving at the last node, the packet is replicated and forwarded to different directions for the rest of each shortest path. Therefore, it enables the packet to be transmitted through the shortest path to each group member, which results in reducing the distribution delay. Furthermore, SPM saves the network bandwidth due to avoiding the duplicate packet transmissions over the common path.

3.2 Assumption and Notation

Since SPM should put the IP addresses of nodes participating in a multicast into the packet header, we assume that SPM is more suitable for the small group applications. Since a node should subscribe to a multicast group membership through a source, it is assumed that all nodes know the IP address of the multicast source. In addition, SPM is provided with the routing path information by ad hoc unicast routing protocols and the path from the source to each node is assumed as the shortest one.

For the description of our SPM, we use the following notations in this paper.

- $G = (V, E)$: G represents the directed graph of a network topology, where V and E are the set of MANET nodes and physical links among the nodes, respectively.
- $p_i = (V_i, E_i)$: p_i is a simple graph. It is a set of nodes on the path from a source to multicast member v_i and the set of physical links E_i to connect those nodes.
- $G_s = (V_s, E_s)$: G_s represents a shortest path tree, where V_s and E_s are the set of nodes and physical links over the shortest path tree;
- $G_m = (V_m, E_m)$: G_m represents a multicast packet delivery tree, where V_m and E_m are the set of all network nodes to participate in a multicast and network-level links among them over an overlay tree, respectively.
- $P = \{ p_1, p_2, \ldots, p_{n-1}, p_n \}$, n is the number of multicast group members.
- $G_1 + G_2 = (V_1 \cup V_2, E_1 \cup E_2)$
- $G_1 - G_2 = (V_1 - V_2, E_1 - E_2)$

– $G_1 \cap G_2 = (\ V_1 \cap V_2,\ E_1 \cap E_2)$
– $outdeg(v)$ = the number of out-going edges from node v.

3.3 Multicast Packet Delivery Tree Construction

The multicast packet delivery tree (G_m) in SPM consists of all network nodes to participate in a multicast (V_m) and network-level links (E_m) among V_m over an overlay tree. The algorithm for multicast packet delivery tree construction has two phases; Shortest-Path-Tree-Creation (SPTC) and Overlay-Creation (OC) (see Algorithm 1.).

Algorithm 1. SPTC–OC Algorithm

Input: The shortest path set P from the source(v_{src}) to each member(V_m)
Output: Multicast overlay tree G_m

1: $P = \{\ p_i \mid p_i$ is the shortest path from the source to multicast member $v_i, 1 \le i \le n$, n is the number of multicast members $\}$
2: $p_{common} = \{\ V_{common},\ E_{common}\ \}$ // p_{common} consist of (V_{common}, E_{common}), where V_{common} is a set of nodes over a tree or path and E_{common} is a set of their edges.

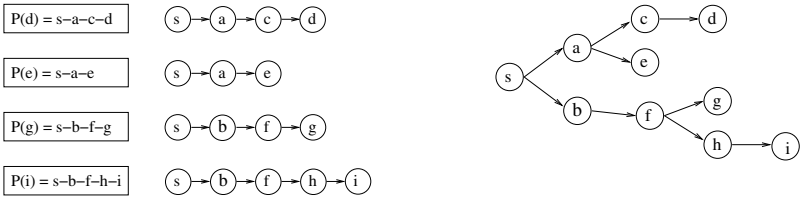
3: In order to acquire G_m, the shortest path tree, $G_s = (V_s,\ E_s)$ is created.
4: $G_s := (\ \{v_{src}\},\ \phi\ )$ // G_s is initialized with $\{v_{src}\}$
5: $V_{JN} := \phi$ // initialize the set of junction nodes.

6: **for** $i := 1$ to n **do**
7: $\quad p_{common} := G_s \cap p_i$ // search for the longest path between G_s with p_i
8: $\quad$ let v_{last} be the farthest element of $\{\ v \mid v \in V_{common},\ v \neq v_{src}\ \}$ from the source.
9: $\quad V_{JN} := V_{JN} \cup \{\ v_{last}\ \}$
10: $\quad G_s := G_s + p_i$
11: **end for**
12: $V_m := V_m \cup V_{JN}$
13: $V_m := V_m - \{\ a \mid outdeg(a) = 1,\ a \in V_s,\ a \notin V_m,\ a \neq v_{src}\ \}$
14: $E_m := \{\ e \mid e$ is a link to V_m at the network layer $\}$
15: $G_m = (\ V_m,\ E_m\ )$
16: **return** G_m

In SPTC phase, at first, the shortest path tree G_s should be found that contains all intermediate nodes over the shortest paths between the source (v_{src}) and each group member. G_s is initialized with ($\{v_{src}\}$, ϕ), where v_{src} is the source node. G_s is expanded in a greedy manner by using the longest common path match. Through the longest common path match, a node can be found at which the common path between G_s and p_i ends (p_i is the shortest path from a source to a multicast member, v_i). The last node over the longest common path is called a junction node (v_{last}). Then, the partial paths from the v_{last} to each

group member which can be reached through the v_{last} are attached to G_s. With the set of paths not included in current G_s, the procedure is repeated until all group members are in G_s.

Figure 2 illustrates an example of the SPTC phase. Suppose the existence of four group members, nodes d, e, g, and i, whose shortest paths from a source, node s, are p_d, p_e, p_g, and p_i, respectively. G_s is initialized with ($\{s\}$, ϕ). Through the longest common path match, the node s is selected as the v_{last} node. Therefore, the partial path toward node d (or p_d) is attached to G_s. Similarly, from the new G_s, the partial paths toward node e (or p_e), node g (or p_g) and node i (or p_i) are attached to G_s in the order.



(a)The shortest paths for group members. (b)The shortest path tree.

Fig. 2. An Example of Shortest Path Tree Construction

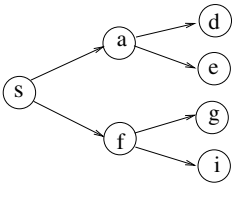


Fig. 3. An Example of Overlay Creation

Through the SPTC phase, we could find the shortest path tree from a source to each group member. Thereafter, when the source multicasts packets, each packet should include a data structure representing the tree in its header. The data structure consists of only junction nodes and group members. Therefore, when each junction node receives a multicast packet, it replicates the packet and forwards it to the corresponding group members or next junction nodes by using its underlying unicast routing protocol as in most overlay-based multicast protocols. Therefore, SPM is interested in the tree whose nodes are junction nodes and group members, not in the tree obtained through the SPTC phase. SPM makes the overlay tree by using OC phase, where the multicast packet delivery tree (G_m) is finally derived by excluding the nodes with one out-going edge from the shortest path tree. Figure 3 shows one example of the tree after the OC phase is applied to Figure 2(b).

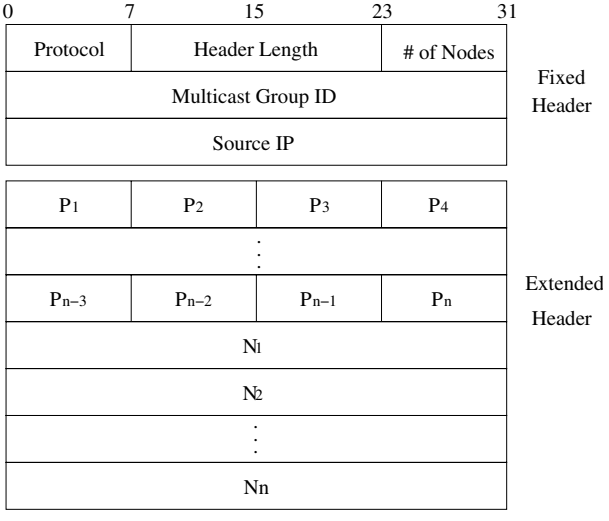


Fig. 4. SPM Header

SPM is currently implemented at application layer. However, since SPM can be extended to be implemented as a thin layer between TCP/UDP and IP, we defined a protocol field in the header. In the case, the SPM message is encapsulated using IP packet. The protocol fields in the IP header and the SPM header indicate the SPM protocol and its upper layer protocol, respectively (see Figure 4). The SPM header particularly represents the overlay tree, which consists of fixed and extension headers. The fixed header includes the source-based multicast session information as well as the number of nodes (the field, # of nodes) which should process the multicast packet (i.e., junction nodes and group members). The extension header includes the data structure, where P_i field in the header indicates the parent node of the field N_i over the overlay tree. P_i is used as an index in the list of the IP addresses. For example, when the P_i value is 2, the parent node of N_i is the node with the IP address of N_2.

3.4 Routing Path Acquisition

SPM needs all routing paths from the source to each multicast member in order to perform the SPTC procedures. In source routing protocols like DSR [6], during the route discovery process, since the RREQ (Route Request) message flooded by a source accumulates the visited intermediate nodes and the RREP (Route Reply) message notifies the source of each accumulated path, the source can easily collect the path information for all group members. However, in case of table-driven routing protocols like AODV [7], since each intermediate node creates a routing entry towards each corresponding member, some modifications to AODV are needed to let the source know the accumulated path information for each group member. While propagating the RREP message which is traversed

over the reverse path towards the source from a receiver, it is enough that the RREP message accumulates the intermediate nodes over the path. Otherwise, like DSR, during RREQ flooding, the path accumulation is performed and it can be returned to the source during the RREP transmission (refer to [4] for the modified RREP message).

3.5 Multicast Join/Leave

This subsection provides a brief overview of the concept of multicast join and leave procedure. As mentioned in Section 3.2, all nodes in the network already know the IP address of a multicast source in advance.

A new node joining a multicast group sends a group join message to the multicast source in a unicast manner. On receiving the join message, the multicast source creates a new multicast packet delivery tree including this joining node by executing the tree construction procedure and replies a join acknowledgement message to the node. When a node wants to leave a group, the node sends a group leave message to the source and the source creates a new multicast packet delivery tree excluding the leaving node. In addition, a periodic tree reconstruction resolves the case that a node left abruptly without sending any leave message gracefully.

4 Performance Evaluation

In this section, we evaluate our SPM and compare it with MAODV using the NS-2 simulator [8]. In Table 1, more simulation parameters are defined.

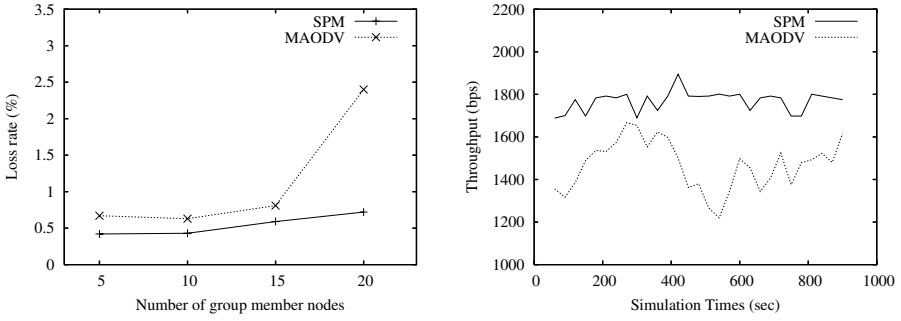
Table 1. Simulation Parameters

Parameter	Value
Total Number of Nodes	50 nodes
Multicast Group Size	5, 10, 15, and 20 nodes
Simulation Area	1500 m x 1500 m
Simulation Time	1000 seconds
MAC Layer	IEEE 802.11b
Packet Size	256 bytes
Traffic Source Type	UDP
Mobility Model	Random waypoint
Node Mobility	1 m/s

4.1 Performance Metrics

We define the following performance metrics.

– *Loss Rate*: A ratio of the number of lost packets to the total number of transmitted packets.



(a) (b)

Fig. 5. Performance Comparison: (a) Loss Rate and (b) Throughput

- *Throughput*: The amount of bits received by each group member per second over simulation time.
- *Distribution Delay*: The time elapsed until every multicast member receives a packet successfully.
- *Average Transmission Delay*: The average time that it takes for each group member to receive a packet successfully.

4.2 Performance Analysis

Figure 5 shows the loss rate and throughput of our SPM and MAODV. In MAODV, since a forwarding node fails to send a multicast packet to its neighbor tree members due to channel contention or node mobility, other group members reachable via the node cannot receive the packet in the event. In particular, note that MAODV needs a reliable multicast MAC protocol for recovering the packet loss at link level. In SPM, although the movement of nodes over paths created from the OC phase can occur and the paths can be broken, the trials to repair the breakage from its underlying unicast protocol allows the packet loss to be reduced compared to MAODV. Since a unicasting utilizes a link-level reliable transmission, the link-level packet loss is recovered by its underlying data link protocol. In addition, since a new shortest path based tree is created in SPM when a new node joins the multicast group, more performance improvement is expected.

Figure 6(a) shows the distribution delay of the SPM and MAODV. Since SPM utilizes the shortest path to each group member, it has less time elapsed until each member receives a multicast packet than MAODV. In MAODV, however, since the shortest path to the existing tree from a joining node is selected, it cannot guarantee the shortest paths from a source to each group member, which results in experiencing more delay.

Due to the similar reasons, SPM showed better performance than MAODV with respect to the average transmission delay as shown in Figure 6(b). However, when the number of group nodes is quite small (for example, 5 nodes in Figure 6),

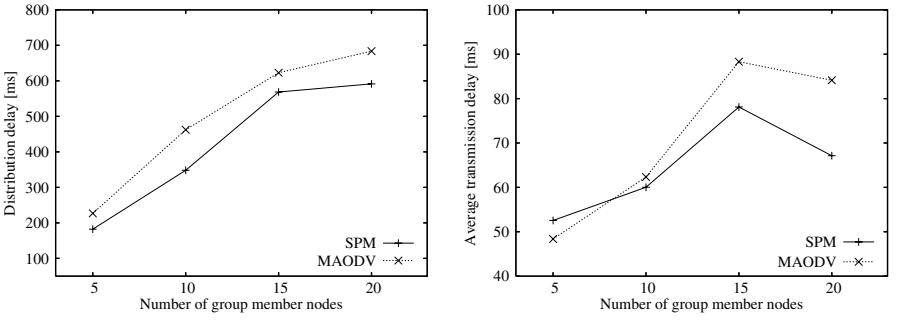


Fig. 6. Performance Comparison: (a) Distribution Delay and (b) Average Transmission Delay

MAODV may have better performance because SPM carries out independent unicasting transmissions for each group member due to lack of the common paths.

5 Conclusion

We investigated the benefits of using an overlay multicasting for small group in mobile ad hoc networks. In this paper, SPM (Shortest Path overlay Multicast) mechanism was proposed, which is suitable for small group multicasting in MANET. SPM utilizes a stateless overlay multicast routing philosophy to avoid the overhead that requires intermediate nodes to manage the membership and routing information. SPM has two phases: Shortest Path Tree Construction (SPTC) and Overlay Creation (OC). In the SPTC phase, a shortest path tree is constructed from the paths provided by an underlying unicast routing protocol. In the OC phase, an overlay tree for an actual multicast packet delivery is created to save the network bandwidth.

Using the acquired overlay tree, SPM multicasts packets over the shortest paths from a source to each group member without duplicate packet delivery over common partial paths. In particular, SPM utilizes the route information provided by ad hoc unicast routing protocol without additional control messages and any other information. By using NS-2 simulator, we proved that SPM shows a better performance than MAODV in terms of throughput, loss rate and packet delivery delay.

References

1. Internet Engineering Task Force, "MANET working group charter," http://www.ietf.org/html.charters/manet-charter.html
2. L. Ji and M. Corson, "Differential Destination Multicast (DDM) - A MANET Multicast Routing Protocol for Small Groups," IEEE INFOCOM 2001, April 2001.

3. K. Chen and K. Nahrstedt, "Effective Location-Guided Tree Construction Algorithms for Small Group Multicast in MANET," IEEE INFOCOM 2002, July 2002.
4. H.-J. Jeong, U. Joung and D. Kim, "Overlay Small Group Multicast Tree Construction Algorithm for MANET," First International Workshop on Network Architecture and Service Models (NASM) 2005, Sanghai, November 2005.
5. E. Royer and C. Perkins, "Multicast Ad hoc On-Demand Distance Vector (MAODV)," IETF Internet-Draft, draft-ietf-manet-maodv-00.txt, July 2000.
6. D. Johnson, D. Maltz and Y. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Internet Draft, draft-ietf-manet-dsr-10.txt, July 2004.
7. C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-demand Distance Vector (AODV) routing," RFC 3561, IETF, July 2003.
8. VINT Group, "UCB/LBNL/VINT Network Simulator ns (version 2)," http://www.isi.edu/nsnam/ns/

Context Awareness in Network Selection for Dynamic Environments*

Daniel Díaz, Andrés Marín, Florina Almenárez,
Carlos García-Rubio, and Celeste Campo

Telematic Engineering Department, Carlos III University of Madrid
Avda. Universidad, 30, 28911 Leganés (Madrid), Spain
{dds, amarin, florina, cgr, celeste}@it.uc3m.es

Abstract. Mobile devices of new generation are able to connect to multiple networks and to constitute new infrastructureless networks. These dynamic environments require new security paradigms and automatic mechanisms to minimize user intervention. Our goal is the definition of a new concept of distance that considers the current domain constraints and the user preferences. This paper addresses some of the problems of these complex environments by using Multidimensional Scaling (MDS) techniques. We also propose collaborative mechanisms for automatic environment marking. Based on these ideas we have developed PervsIM, a decision mechanism that selects the most appropriate network or peer to interact with. Besides we have defined an embedded access control module which ensures that PervsIM decisions are followed by all applications. Furthermore, several simulation results and implementation details outline how these results can be incorporated in today's mobile devices.

Keywords: Context, network selection, trust, access control.

1 Introduction

Wireless network technologies are evolving providing more coverage, speed and quality of service. Moreover, the cost of the technology is decreasing so that it benefits the deployment. As a consequence, the number of mobile devices increases. Mobile devices are also enhancing their network support, being usually shipped by manufacturers with different network interfaces, like IrDA, bluetooth or WiFi. This enables them to connect to multiple networks and to constitute new infrastructureless networks.

In dynamic environments it is desirable that devices can be grouped defining domains. Grouping devices in domains makes it easier to determine, where we are, how closer the devices of a domain are and what we can do within a domain.

* This work has been partially supported by Everywhere (MCyT N2003-08995-C02-01) and by grant UC3M-TEC-05-056 of the Program to Support the Creation and Consolidation of Universidad Carlos III Research Groups.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 216–227, 2006.

In this paper we outline a mechanism to determine "where we are" by collecting context information and the unique IDs of access points and static devices. Currently, mobile devices require human input either from final users or providers to mark networks, access points or peers. The marking information helps the mobile device to select among the (growing) list of preferred networks. In this paper we propose an automatic mechanism of collaborative marking, which allows setting up marking information without user intervention for devices in a domain.

We also depict "what we can do" by defining policies. The mark given to domain devices, used together with the policies, parameterize the behavior. We also propose to embed the access control mechanisms in the operating system so even legacy applications can be controlled.

Moreover, when mobile devices switches on, or moves to other places it is necessary to select the appropriate network or peer to interact in order to satisfy user needs or, for example, if it is roaming, to reduce handoff delay (make-before-break). Deciding the peer, network, or entity to interact with, may be conditioned by multiple factors. Humans tend to consider multiple factors when deciding but, as a last resort, tend to simplify problems. Thus, why do not implement decision engines that simplifies such decisions?. This paper address the problem of selecting the most appropriate network or peer to interact with, defining a new concept of distance that considers the current domain constraints and the user preferences.

Section 2 introduces the problem domain, and the previous works are described in section 3. Section 4 outlines the prototype: domain definition and marking, policy manager and finally, the decision engine where it will be shown how multidimensional scaling, a psychometric algorithm, helps to alleviate decision problems. Section 5 gives implementation details, and finally section 6 present the conclusion and future work.

2 Motivation

Marc Weiser stated that "*the most profound technologies are those that dissapear*" [1], meaning that the user is not aware of them. Context awareness and processing is definitely needed to operate under the consciousness level of human. Moreover, intuitive ways of displaying context information, even mimicking human thinking are desirable capabilities for the technologies described by Weiser.

Satyanarayanan said that interactions in pervasive computing environments decay with the square of distance [2]. This statement applies to every interaction since the energy of signals decays in the same fashion. The goal of Satyanarayanan is to establishes a way to measure what can be called *interaction distance*. But, what about other metric or non metric attributes as trust, economic cost, type of service and any other defined by the user? Shall them be taken into account when selecting an appropriate peer to interact with? How can we assist the user in selecting the network with the least interaction distance, and do this *invisible* to the user?

There are other works that focus on network services, providing security and service continuation for wireless communications [3], and [4], but do not take into account the network selection problem. MDS data analysis techniques have been used for several problems with good results. [5] shows how MDS can be used to determine the distance among elements of sensor networks that takes $O(n^3)$ time to find a solution. A mechanism based in MDS is described in [6] to classify music, browse it and generate playlists.

Limited devices, specially personal devices, are very rich in context information. They can hold information on user location, and user personal information like the agenda, or the contacts list. This work presents a solution for assisting users to select the best network according to their preferences.

From the point of view of applications using the network, the selection process is part of the access control protecting the resource *network access*. In this paper we are focusing on network access as the resource to be protected: we want to ensure that applications use the most appropriate network available at each moment. We will introduce the context information available for personal devices into the access control.

For the selection process, we will take into account valuable context information including location, trust, and cost, process it according to the user preferences, and take the decision or alternatively present the context information to the user in a comprehensive way using MDS.

3 Previous Work

3.1 Pervasive Trust Manager

Pervasive Trust Manager (PTM) allows to manage ad-hoc relationships with other peers in a secure way (see [7]). This manager has been designed for personal devices that act as autonomous peers, belonging to different trust domains. These autonomous peers protect their own resources and communicate securely with each others.

PTM benefits from the common knowledge in the environment. Such knowledge is obtained from close peers, which recommend other known peers. This information is exchanged using a Pervasive Recommendation Protocol (PRP). Devices derive their own opinion about third peers from the recommendations. Such opinions are expressed using fuzzy logic and are calculated taking into account both recommendation data and the trust data about the recommenders. PTM keeps trust data about third peers, which are identified by their public key. It stores both trust and distrust information. After the formation of an initial opinion, PTM takes into account the behaviour of entities to vary the trust data and consequently the opinion.

3.2 Multidimensional Scaling

Multidimensional Scaling [8], MDS, is a set of techniques widely used in behavioral, psychologic and econometric sciences to analyze similarities of entities.

From a pairwise dissimilarities matrix, usually m-dimensional Euclidean distances [5], MDS can be used to represent the data relations faithfully providing a geometrical representation of these relations. MDS is used to reduce the dimensionality of a problem to a small value.

MDS can consider not only Euclidean distances but also any other evaluation of the dissimilarities of the entities. Dissimilarities can be classified according to whether the data is qualitative or quantitative. The dissimilarities from attributes of data can be weighted (weighted MDS), thus, assigning a different weight to each attribute allows to obtain more particular results depending on the problem. So, a complex m-dimensional problem can be simplified preserving the essential information using MDS.

There exists a multitude of variants of MDS with slightly different cost functions and optimization algorithms. The first MDS for metric data was developed in the 1930s and later generalized for analyzing nonmetric data [9].

In classical scaling the proximities are treated as distances, however, any (di)similarity can be derived from data attributes in order to obtain a metric, but it is necessary to hold the properties of non-degeneracy (diagonal elements should be zero, $d_{i,i} = 0$) and triangular inequality that states that $d_{i,j} + d_{i,k} \geq d_{j,k}$ for every i, j, k. The distance between two points i and j in a m-dimensional Euclidean space is defined as follows:

$$d_{i,j} = [\sum_{a=1}^{m} (x_{i,a} - x_{j,a})^2]^{\frac{1}{2}} \tag{1}$$

For Euclidean distances, distances $d_{i,j}$ are related to the observed proximities $p_{i,j}$ by an appropriate transformation $d_{i,j} = f(p_{i,j})$, depending on the measurement characteristics. A linear transformation, $d_{i,j} = a + bp_{i,j}$, can be assumed for unique distances with $b < 0$ for similarities and $b > 0$ for dissimilarities.

If the solution is derived using least-squares, a linear transformation of proximities $I(P)$ can be defined as $I(P) = D + E$, with D the distances matrix (that is a function of the coordinates) and E the residual error. The solution obtained is the X such the sum of squares of E is minimized. The double centered matrix of scalar products, B, can be defined as $B = XX^T$ where X is the coordinate matrix. The value of B is:

$$B = -\frac{1}{2}[I - \frac{1}{n}ii^T]D^2[I - \frac{1}{n}ii^T] \tag{2}$$

where n is the number entities, I an $n \times n$ identity matrix and i a unity vector of length n. Decomposing the matrix B into its singular values, $B = VAV^T$, the coordinate matrix X can be calculated as $X = VA^{\frac{1}{2}}$.

To reduce the complexity of a m-dimensional problem, we can choose $l < m$ eigenvalues and eigenvectors. Taking only the largest l eigenvalues and eigenvectors the problem is simplified to a l-dimensional problem.

However, in case of ordinal data, another procedure has to be followed than the use of singular value decomposition since we want to recover the order of the proximities and not the proximities or a linear transformation of the proximities.

A solution to this problem was given by Shepard [10] and refined by Kruskal [11]. These solution iteratively minimize a fit measure called *Stress* by an iterative algorithm, which is suitable for processing.

We have used an algorithm called ALSCAL [12], which uses alternate least-squares, combined with weighted (di)similarities, for simulation and implementation. ALSCAL finds a local minimum and can be used for both metric and nonmetric analysis. Furthermore, the ALSCAL algorithm can also deal with spare proximity matrixes so it is suitable for simplify problems in the absence of some data.

4 Pervasive Interaction Manager

The Pervasive Interaction Manager (PervsIM) is the solution we propose to address the aforementioned problems. PervsIM is composed by four modules: the domain definition module, the collaborative domain marking module, the policy manager and decision engine.

The prototype is described through this section. A brief description of some concepts may help the reader to understand better what is addressed in this section. **Devices** are grouped together in **domains**. The closest set of devices that surround us is considered the current **domain**. Devices within a domain are divided in static devices, called **anchors** and moveable devices called **peers**.

4.1 Domain Definition Module

This module is in charge of determining the current environment and grouping devices together in domains. The major constraint of interaction is the physical distance [2] since the energy of signals decays with the square of its value. So, the nearest set of devices define the current domain. The module uses the mentioned relative localization and neighbor information to define an domain.

Given a domain, the static wireless devices within that domain, for instance, network access points, printers and screens can be uniquely defined by their MAC address or other cryptographical identifier and considered as **anchors** or reference points. The anchors of a domain help the mobile device to recognize the domain as known.

For every element of the domain, the module finds out the attributes that will be used to compute the *interaction distance*. The attributes represent context information (quantitative, ordinal or category membership information) that depend on the user preferences (see section 4.4). The type and number of attributes are user-defined, but at least, two should be considered: physical distance and trust value. Besides, other attributes like service information from discovery protocols [13] (if applicable), required credentials, or economic cost, can be considered.

Physical distance is derived using received signal strength measures. The module takes values for the received signal strength from each network access point or anchor. Once out of bound anchors are deprecated, the signal strength is

scaled by a factor, that depends on the network interface technology, in order to provide a normalized value within 0 and 1.

Furthermore, localization techniques using signal strength provide good privacy and are inexpensive: radio hardware is used not only to establish communications, but also to determine the relative position. The accuracy of signal strength localization techniques is limited and decrease even more in indoor environments [14] [15], however, network interfaces are enough to uniquely determine the current domain by using unique identifiers and to determine if the mobile node is approaching or moving away from that domain.

The trust value for each element of the domain is handled by PTM (section 3.1), for ad-hoc elements, and by the collaborative domain marking module (section 4.2) for anchor elements.

Obviously, the domain borders are rouge but, combining all the attributes, a useful measure of *interaction distance* can be derived and used to take decisions (section 4.4). Finally, the aforementioned attributes are stored as XML elements. These elements contains, at least, the necessary information to identify that domain (anchors) and a time-to-live value.

4.2 Collaborative Domain Marking Module

The aim of this module is to automatically give marks to domain anchors, instead of asking the user for that information, other peers are asked for opinion. The anchors and attributes that define a domain can be different even for the nearest peers. So that, when two peers exchange information they only consider what they have in common. In general, several attributes can be exchanged among peers to compute a mark, but currently, information exchange is restricted to trust values but the model is opened.

The process is simple, trust values are exchanged securely among peers, and scaled by a factor that depends on the trust value assigned by PTM to the recommender peer. The peer i uses the received information from peer k to compute a value, $\beta_{i,j}$, which is the trust value that peer i has for an anchor j. The peer i quantify its trust to another peer k with a value among 0 and 1, $\alpha_{i,k}$, and it only accepts recommendations from peers with a trust value higher than α_{min}. The trust value $\beta_{i,j}$ increment for the n^{th} recommendation is calculated using the following expression:

$$\Delta\beta_{i,j} = \frac{\alpha_{min}}{n \log n}(\beta_{k,j} - \beta_{i,j})\alpha_{i,k} \quad \forall \quad (\alpha_{min} < \alpha_{i,k}) \tag{3}$$

$$\Delta\beta_{i,j} = 0 \quad \forall \quad (\alpha_{min} > \alpha_{i,k}) \tag{4}$$

The marking module uses a scale factor that permits an initial fast increment of the trust value for an anchor, but avoid collaborative attacks since its value decreases with the number of recommendations. This scale factor can be customized by the user. Fig. 1 shows the evolution of the trust value for an anchor using a scale factor of $\frac{\alpha_{min}}{n \log n}$.

As can be seen in Fig. 1, the results are conditioned to the value of α_{min}. This is a very conservative approach like used in reputation systems, which

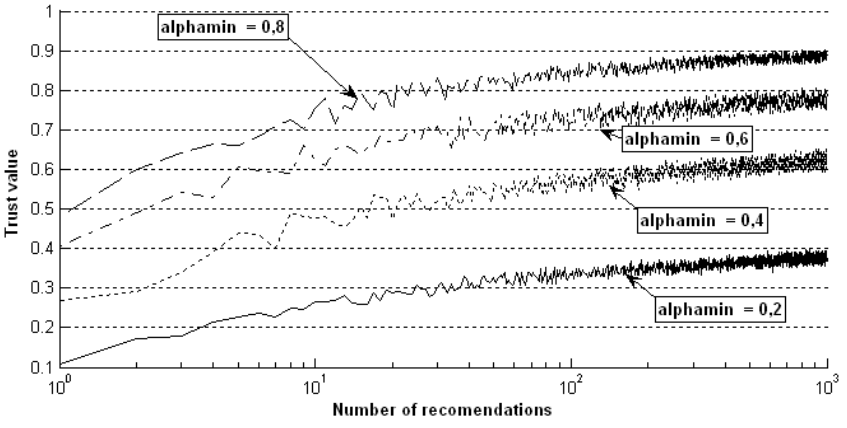


Fig. 1. Anchor trust value evolution from 0 vs number of recommendations. Recommended value 1.0.

tend to protect against malicious recommendations. The higher the value of α_{min} is, the higher trust value can be reached but the less recommendations are taken into account ($\alpha_{i,k}$ should be grater that α_{min}). Besides this model, others have been considered. A less conservative approach will be using $\frac{\alpha_{i,k}}{n \log n}$, so that recommendations coming from high trusted recommenders influence more our final trust value.

This mechanism allows to automatically derive a trust value for new environments that helps the mobile device to identify trusted or distrusted environments and behave in consequence as depicted in section 4.3.

4.3 Policy Manager Module

Limited devices host resources subject of protection, in this way, we use a policy manager to made access decisions based on policies. Access control policies allow defining a dynamic and semi-automatic mechanism of protection, in order to adapt our applications to the context and to minimize the user intervention.

A generic access control system has been previously defined in [16], so in this work, we include a specific application for controlling the access to the network interfaces. Such system is based on the XACML standard [17] to define the policies and the exchange of information.

XACML defines an architecture for access control in web systems comprising PCs and servers. It is a flexible approach which allows to specify different policies and rules which can be later evaluated by the Policy Decision Point (PDP) to permit or deny access to resources. Requests to resources should be trapped by the Policy Enforcement Point (PEP), to avoid malicious entities from bypassing

the access control. The collaboration among PEP and PDP ensures the access control is performed. Regarding the PEP there are two main approaches: either the PEP is included in the applications, or the applications access the PEP via an API to ensure correct access control. Nevertheless, non-cooperating applications or even malicious like virus, trojan horses, and the like, could circumvent the PEP and access the resources directly. One possible solution we propose here is to implement the PEP at the operating system (kernel) level, making unauthorized access more difficult to such kind of applications. Besides, it ensures that the applications shipped by the manufacturer also comply with the access control.

We benefit of the flexibility of XACML, extending the attributes to include trust data, and external context information. So, the decisions are made based on the trust assigned to other peers and available context information such as location, user preferences, or even cost.

4.4 Decision Engine Module

Multidimensional scaling techniques (section 3.2) are used in this module to find an ordered sequence of peers (including access points) to interact with, depending on the user preferences. The problem of deciding which is the best network or peer in complex environments is addressed by using techniques that allows the mobile device to *simplify problems as humans do*. Thus, a simple measure of what can be called *interaction distance* is derived for every peer using all the available information.

Consider an environment with many anchors and peers (elements). (Di) Similarities between pairs of elements can be derived as follows:

$$\delta_{i,j,\alpha} = \frac{|u_{i,\alpha} - u_{j,\alpha}|}{max(u_\alpha) - min(u_\alpha)} \quad for\ quantitaive\ data \tag{5}$$

$$\delta_{i,j,\alpha} = \frac{|rank(u_{i,\alpha}) - rank(u_{j,\alpha})|}{max(rank(u_\alpha)) - 1} \quad for\ ordinal\ data \tag{6}$$

$$\delta_{i,j,\alpha} = \begin{cases} 0 : u_{i,\alpha} = u_{j,\alpha} \\ 1 : otherwise \end{cases} \quad for\ category\ mebership\ data \tag{7}$$

where $u_{i,\alpha}$ is the α^{th} attribute value of the peer i. We consider data of different nature: quantitative data is used, to describe trust relations (section 3.1) and distances [5]; ordinal data for QoS classes, and to distinguish among different services; membership data help to classify elements, for example, ad-hoc peer or infrastructure network access point.

Once the (di)similarities are calculated they are weighted with the user preferences in order to obtain an unique weighted (di)similarities matrix. These weighted (di)similarities are defined for a set of n objets with q attributes as follows:

$$\delta_{i,j} = \left(\frac{\sum_{\alpha=1}^{q} w_{i,j,\alpha} w_\alpha \delta_{i,j,\alpha}^{\lambda}}{\sum_{\alpha=1}^{q} w_{i,j,\alpha} w_\alpha}\right)^{\frac{1}{\lambda}} \tag{8}$$

where $w_{i,j,\alpha}$ takes value 0 if objects i and j can not be compared on the α^{th} attribute and 1 otherwise, w_α is the weight given by the user to attribute α and $\delta_{i,j,\alpha}$ is the (di)similarity between objects i and j on the α^{th} attribute.

Although the model can include any other context relevant information, Table 1 shows a possible scenario for a user that measure the *interaction distance* in terms of trust (a value between 0 and 1), distance (derived from received signal strength) and economic cost. The first element represents the ideal element that will be used to measure the *interaction distance*: it has a trust value of 1, is very close to the device (distance 0) and interactions are free. Using the MDS ALSCAL algorithm, solving for one dimension and setting $\lambda = 2$ to handle attributes as distances, it is possible to derive a value for the *interaction distance* between the ideal element and the others, and also classify the elements. In this table we show the attribute values $u_{i,\alpha}$ for every element.

Table 1. Attribute values in a possible decision scenario

	Ideal(1)	2	3	4	5	6	7	8	9	10	11
Trust	1.0000	0.9429	0.8430	0.9573	0.8344	0.0206	0.0464	0.0075	0.0597	0.0191	0.0935
Distance	0	0.5259	0.5048	0.4633	0.5270	0.4757	0.5635	0.2540	0.2587	0.2509	0.2670
Cost	0	0.2054	0.2738	0.8636	0.8931	0.8461	0.8513	0.8424	0.8416	0.0	0.0

In the example we consider two situations: for the first one, the policy establishes the weights vector $Trust, Distance, Cost = 0.8, 0.1, 0.1$. The decision engine provides an ordered list of elements that meet this criteria and the distance to the ideal element 1. In Fig.2 there is a pair of representations of this decision for one and two dimensions. The axis of the figure do not represent any criteria, the figure just represent how closer elements are from each others. The result of this decision is $1, 4, 2, 5, 3, 11, 9, 7, 6, 10, 8$. Examining the results it can be seen that peers can be divided in two groups, the peers of the first group $(4, 2, 5, 3)$, since are close to the ideal element 1, are eligible. The others, are grouped together far from the ideal element, so are not eligible peers.

In the second situation, (Fig. 3) the policy establishes the weights vector $Trust, Distance, Cost = 0.1, 0.8, 0.1$. The result, $1, 10, 11, 8, 9, 6, 4, 3, 2, 5, 7$, shows that the distance between the ideal element 1 and the closest group 10,11,8,9 is very high so the mobile device may decide not to interact.

Weights vectors for the example have been exaggerated for a better understanding. In general, other more reasonable criteria can be easily considered.

The simulations we have performed show that the model suits the data. ALSCAL minimize a parameter called S-STRESS that is used to stop the iterations when its value is lesser than a minimum. The average of S-STRESS obtained in the simulations (varying the number of elements from 2 to 60) is 0.2728 and the results seem to be useful. Perhaps, stopping the iterations for this S-STRESS value is not suitable for other data analysis problems that need more accuracy, but it is enough for the network selection problem and less resources are consumed. Moreover, the quadratic correlation between the (di)similarities

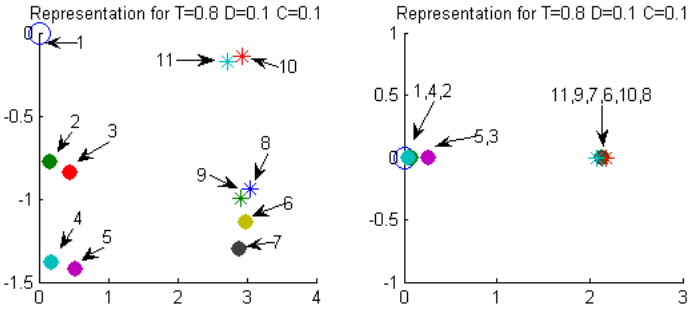


Fig. 2. Access point (anchor) selection favoring trust (Trust 0.8, Distance 0.1, Cost 0.1)

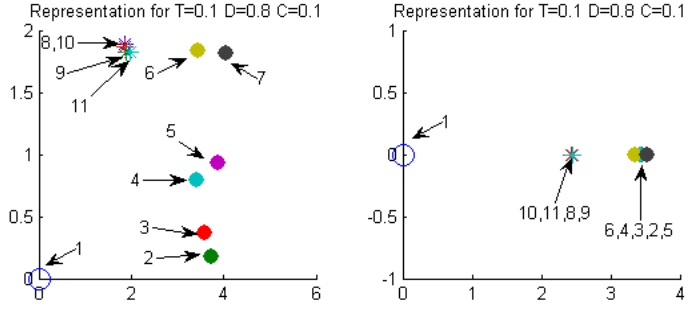


Fig. 3. Access point (anchor) selection favoring distance (Trust 0.1, Distance 0.8, Cost 0.1)

and the distances (RSQ), is a parameter that gives and idea of the goodness of the fit, 1 for a perfect fit and 0 for the worst fit. The model provided values for RSQ between 1 and 0.8. The complexity of the algorithm is $O(n^{2.65})$ where n is the number of elements.

5 Implementation Details

To validate our design, we have developed a prototype for Windows Mobile operating system. Windows Mobile, a Microsoft operating system, derives from Windows CE.

The implementation have been done in C++ under Windows Mobile. To gather information about anchors we have used the results of the Herecast project [18], a set of libraries that interact with the Network Device Interface System (NDIS), present in every Windows based operating system, that provides localization-based WiFi services.

We have implemented two Policy Enforcement Points (PEP) for handling legacy applications interactions. One of the PEPs controls the network traffic: the Network PEP (NPEP). The other controls the use that secure protocols, as SSL or TLS, make of the available credentials: the Secure PEP (SPEP).

When either an outgoing or an incoming connection takes place it is detected through the NPEP. The NPEP analyzes the destination, origin and protocol. Then, the NPEP provides that information to the Policy Decision Point (PDP).

The NPEP is a NDIS intermediate driver that is placed on the top of the NDIS miniport drivers but behind the NDISUIO driver. The PEP have bindings to all the network interface drivers below it so it can sniff the incoming and outgoing traffic and provide this information to the PDP. Thus, the PDP can allow or deny a particular interaction depending on the domain even for legacy applications.

The PDP not only decide when it is triggered by an application request, but also it can take decisions depending on the context changes. To select among the different network interfaces the PDP uses the NDISUIO driver [19] that is a connection-less, NDIS 5.1 compliant protocol driver. Using this intermediate driver, the PDP module can establish and tear-down bindings to network adapters.

Thus, depending on the domain, some network interactions can be allowed or not, i.e. if the mobile device is in a distrusted domain the policy module can either tear-down all the bindings, to deny connections, or set filters for some protocols for incoming and outgoing traffic. The PDP uses an XACML engine.

6 Conclusions and Future Work

The solution depicted in this paper provides mechanisms that allow a mobile device to take decisions based in the environment. The decisions are driven by policies that consider both user preferences and environment information. We have focused on attributes as trust and distance but we have shown also that many others can be considered.

We have demonstrated also how multidimensional scaling algorithms, that helps to think as humans, are useful to simplify decision problems with a complexity of $O(n^{2.65})$. Other algorithms that minimize different cost functions than ALSCAL will be tested to improve performance.

We are now facing the validation phase of the work. Our next step is to test the solution in different environments to measure the load and the resource consumption. We are planning also to move the solution to Symbian mobile phones.

References

1. Weiser, M.: The computer for the 21st century (1991)
2. Satyanarayanan, M.: Pervasive computing: Vision and challenges. IEEE Personal Communications **8** (2001) 10–17 citeseer.nj.nec.com/gennaro99robust.html.

3. Dutta, A., Zhang, T., Madhani, S., Taniuchi, K., Fujimoto, K., Katsube, Y., Ohba, Y., Schulzrinne, H.: Secure universal mobility for wireless internet. In: WMASH. (2004) 71–80
4. Chaouchi, H., Pujolle, G., Armuelles, I., Siebert, M., Carlos Bader, F., Ganchev, I., ODroma, M., Houssos, N.: Policy based networking in the integration effort of 4g networks and services. In: Proceedings of IEEE Semiannual Vehicular Technology Conference (VTC2004-Spring), Milan, Italy (2004) 5
5. Shang, Y., Ruml, W., Zhang, Y., Fromherz, M.P.J.: Localization from mere connectivity. In: MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, New York, NY, USA, ACM Press (2003) 201–212
6. Platt, J.C.: Fast embedding of sparse music similarity. In: Advances in Neural Information Processing Systems vol. 16. (2004)
7. Almenárez, F., Marín, A., Campo, C., García, C.: PTM: A Pervasive Trust Management Model for Dynamic Open Environments. In: First Workshop on Pervasive Security, Privacy and Trust PSPT'04 in conjuntion with Mobiquitous 2004. (2004)
8. Borg, I., Groenen, P.: Modern multidimensional scaling, theory and applications. In: IEEE SECON 2004, New York, NY, USA, Springer-Verlag (1997)
9. Deun, K.V., Delbeke, L.: Multidimensional scaling (2000) http://www.mathpsyc.uni-bonn.de/index.htm.
10. Shepard, R.N.: The analysis of proximities: multidimensional scaling with unknown distance function part i. In: Psychometrika 27. (1962)
11. Kruskal, J.B.: Multidimensional scaling by optimizing goodness of fit to a nonmetric hypothesis. In: Psychometrika 29. (1964)
12. Takane, Y., Young, F.W., de Leeuw, J.: Nonmetric individual differences multidimensional scaling: an alternating least squares method with optimal scaling features. In: Psychometrika 42. (1977)
13. Campo, C., García-Rubio, C., Marín, A., F.Almenárez: PDP: A lightweight discovery protocol for local-scope interactions in wireless ad hoc networks. Computer Networks Journal. Elsevier (2006) Pending to be published.
14. Elnahraway, E., Li, X., Martin, R.P.: The limits of localization using rss. In: SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, New York, NY, USA, ACM Press (2004) 283–284
15. Elnahraway, E., Li, X., Martin, R.P.: The limits of localization using signal strength: a comparative study. In: IEEE SECON 2004. (2004) 406–414
16. Almenárez, F., Marín, A., Campo, C., García, C.: TrustAC: Trust-based access control for pervasive devices. In: 2nd International Conference Security in Pervasive Computing (SPC'05). (2005)
17. OASIS: eXtensible Access Control Markup Language (XACML) (2003) http://www.oasis-open.org/apps/org/workgroup/xacml/.
18. Paciga, M.: An open infrastructure for location-based services using wifi (2005) http://www.herecast.com.
19. Microsoft: Ndisuio: Ndis user mode i/o (2005) http://www.ndis.com/pcakb/KB01010301.htm.

A Secure Global State Routing for Mobile Ad Hoc Networks

Chen Jing[1], Cui Guo Hua[1], and Hong Liang[1]

[1] College of Computer, Huazhong University of Science & Technology Wuhan 430074, China
ever_cs@smail.hust.edu.cn

Abstract. The secure operation of the routing protocol is one of the major challenges to be met for the proliferation of the Mobile Ad Hoc networking (MANET) paradigm. Secure Global State Routing Protocol (SGSR) proposed here defines some rules to ensure secure neighbor discovery. Priority is introduced to prevent denial of service attacks. SGSR also can limit the packet in a certain area. So it can be employed as a stand-alone protocol, or fit naturally into a hybrid routing framework. This paper provides formal analysis to illuminate that SGSR is robust against individual attackers. The simulation result shows that the efficiency and the cost of the protocol are in an acceptable scope after adding the secure mechanisms.

Keywords. Ad Hoc; Network Security; Routing Protocol.

1 Introduction

The Mobile Ad Hoc Networking (MANET) has the collaborative, self-organizing environment. It opens the network to numerous security attacks that can actively disrupt the routing protocol and disable communication[1]. Recently, many ad hoc routing protocols have been proposed. Most of the protocols discover the route only when a source node needs to route packets to a destination node; that means, they are reactive routing protocols[2]. But in many situations, proactive discovery of topology performs better. Link State Routing protocol(LSR) is a "proactive" routing scheme. SGSR is based on LSR.

Some vicious nodes may exhibit some malicious behaviors, such as: forgery, replay, corrupting link state updates or Denial of Service (DoS) attacks. This paper provides a scheme to secure the discovery and the distribution of link state information. Section 2 takes a look at related work. Section 3 presents our Secure Global Routing Protocol and the data that nodes need. Section 4 and 5 provide the security and formal analysis. Section 6 shows the result of the simulation. Finally, it concludes with a description related to future work.

2 Related Work

The collaborative, self-organizing environment of the Mobile Ad Hoc Networking technology opens the network to numerous security attacks that can actively disrupt

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 228 – 238, 2006.

the routing protocol and disable communication. Attacks on ad hoc network routing protocols generally fall into one of two categories: 1) Routing-disruption attacks. The attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. 2) Resource-consumption attacks. The attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth or to consume node resources such as memory (storage) or computation power.

Recently, a number of protocols have been proposed to secure wireless ad hoc routing. Papadimitratos and Haas proposed the SRP (Secure Routing Protocol)[6], which we can use with DSR (Dynamic Source Routing Protocol) or the Interzone Routing Protocol in the ZRP (Zone Routing Protocol). They designed SRP as an extension header that is attached to ROUTE REQUEST and ROUTE REPLY packets. SRP doesn't attempt to secure ROUTE ERROR packets but instead delegates the route-maintenance function to the Secure Route Maintenance portion of the Secure Message Transmission protocol. SRP requires that, for every route discovery, source and destination must have a security association between them. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected, and any malicious node can just forge error messages with other nodes as source. Ariadne [12] is a secure on-demand routing protocol based on DSR and TESLA(Timed Efficient Stream Loss-tolerant Authentication), which withstands node compromise and relies on highly efficient symmetric cryptography and requires clock synchronization. ARAN(Authenticated Routing for Ad hoc Networks) is based on AODV(Ad hoc On-Demand Distance Vector Routing Protocol) and proposed by Dahill. In ARAN, each node has a certificate signed by a trusted authority. Every node that forwards a route discovery or a route reply message must also sign it, which is very computing power consuming and causes the size of the routing messages to increase at each hop.

3 Secure Global State Routing Protocol(SGSR)

The scope of SGSR may range from a secure neighborhood discovery to a network-wide secure link state protocol. SGSR nodes distribute their link state updates and maintain topological information within R hops, which we refer to as zone.

3.1 Node's Equipment

Node i is equipped with a public/private key pair, namely K_i and K_i^{-1} . Key certification can be provided by a coalition of N nodes and the use of threshold cryptography[4].

We assume that network links are bidirectional, which means if node A is able to transmit to node B, then B is also able to transmit to A. we also assume that wireless interfaces supporting promiscuous mode operations. Every node is identified by its IP addresses, which can be assigned by many schemes, e.g., dynamically or even randomly. But after the node enters the network and passes the authentication, IP address becomes unchangeable.

Every node has a neighbor information table as table 1:

Table 1. Neighbor information table

IP_i	K_i	SEQ_i	K_{TC}	$Cert_i$

In order to explain SGSR clearly, we define some symbol as table 2.

Table 2. Symbol definition

IP_i	The IP address of node i	MAC_i	The MAC address of node i
K_i	The public key of node i	K_i^{-1}	The private key of node i
$Cert_i$	The Certification of node i	SEQ_i	The sequence of node i
K_{TC_i}	The single hop broadcast key of node i	$\{X\}K$	Using key K to encrypt or decrypt X
$H(X,K)$	Using key K and X to calculate hashing value	$K_{TC\_i}^{j}$	Node j 's K_{TC_i}

3.2 Neighbor Detecting

Each node submits a pair of its (MAC_n, IP_n), to its neighbors by broadcasting hello messages. If node A considers the hello packet coming from a legal node, it will accept the packet and update the neighbor information table. But if node A finds the packet is initiated by a strange node B, it will launch an authentication process.

Because the cost of calculating a hash value is smaller than signature, SGSR uses a single hop broadcast key to ensure the authenticity and integrality of the packets. Each node must exchange the single hop broadcast key to its neighbor together with authentication. N_a is a random number created by A. The process is as follow:

(1) $A \rightarrow B : Cert_A, \{N_a\}_{K_A^{-1}}$

(2) $B \rightarrow A : \{K_{TC\_B}, N_a + 1\}_{K_B^{-1}}, Cert_B$

(3) $A \rightarrow B : \{K_{TC\_A}, N_a + 2\}_{K_A^{-1}}$

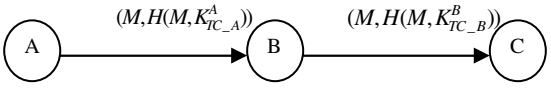


Fig. 1. *A* transmit packets to *C*

Neighbor Detection has the following tasks:

(1) Maintaining the neighbor information table: if neighbor changes IP or uses other IP, deletes the neighbor from the neighbor table.

(2) Judging latent discrepancies, such as a single data-link interface using multiple IP addresses.

(3) Measuring the rates at which control packets which are received from each neighbor, by differentiating the traffic primarily based on MAC addresses, if one neighbor's sending rate is too high, SGSR debases its packets' priority.

3.3 Secure Forwarding Packets

There are three nodes named *A*,*B*,*C* shown in fig.1. *B* is the neighbor of *A* and *C* while *A* and *C* are not neighbors. *A* sends packets to *C*. *M* denotes the packet's content.

(1) $A \rightarrow B : (M, H(M, K^A_{TC\_A}))$

(2) Node *B* uses *M* to calculate $H(M, K^B_{TC\_A})$, if $H(M, K^A_{TC\_A}) == H(M, K^B_{TC\_A})$, goto (3), else drops the packet.

(3) $B \rightarrow C : (M, H(M, K^B_{TC\_B}))$

(4) Node *C* uses *M* to calculate $H(M, K^C_{TC\_B})$, if $H(M, K^B_{TC\_B}) == H(M, K^C_{TC\_B})$, accepts the packet, else drops the packet.

Because the single hop broadcast is created by the process authentication, the malicious node can't get the single hop broadcast key. This method is more effective than using signature but keeps the same security.

3.4 Global State Update and Hops Limitation

Global State Updates (GSU) are identified by the IP address and the SEQ. The SEQ, a 32-bit sequence number, provides the updates from an address space of four billion. The structure of the Global State Updates is composed of eight parts that are shown in fig.2.

TYPE stands for the type of packet, R_{HOPS} indicates the number of the hops that the Global State Updates Packet has traveled; RESERVED denotes the field reserved;

HASH_MAXHOPS indicates the hash value[5] of the max hops, *HASH_TRAVERSED* denotes the hash value now, *GSU_SEQUENCE* indicates the sequence of the Global State Updates Packet, NEIGHBOR_TABLE denotes the neighbor information table of the sender, SUMMARY can prevent the malicious node juggling using the method of section 3.3.

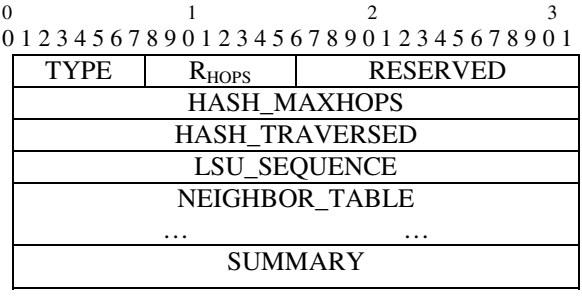


Fig. 2. Global state updates packet (broadcast the state of the node's neighbor)

R_{HOPS}, *HASH_MAXHOPS*, *HASH_TRAVERSED* are used for limiting the max hops and avoiding flooding. The arithmetic is as follow:

(1) If a node sends the Global State Updates packet, goto (2), and if it forwards the packet, goto (4).

(2) The node sending the packet chooses a random value V, and calculates a hash chain, $H^0(V)=V$,$V_i = H^i(V)$, $i=1,...,N$. N is the max number of hops allowed. $H^i(V)$ means the hash value after i times calculated with the parameter V.

(3) *HASH_TRAVERSED* is equal to V_0 and *HASH_MAXHOPS* is equal to V_N, goto (7).

(4) The node receiving the packet validates the SUMMARY . If it fails, goto (8), else goto (5).

(5) The node uses the *HASH_TRAVERSED* in the received packet to calculate the value of $H^{N-R_{HOPS}}(HASH\_TRAVERSED)$, if the value is equal to *HASH_MAXHOPS*, then goto (6), else goto (8).

(6) The *HASH_TRAVERSED* is replaced by *H(HASH_TRAVERSED)*, and R_{HOPS} is replaced by $R_{HOPS}+1$.

(7) The node sends or forwards the packet. The process ends.

(8) The node drops the packet. The process ends.

4 Security Analysis

MANET may be suffered from two types of attack. One is active attack. The attackers achieve their illegal aim by modifying, deleting, delaying, inserting the data stream. The other is passive attack[6,7]. The attacker only listens to the information in the network, instead of modifying it. SGSR is effectual when the attack is active.

The attacks which SGSR can resist are as follows:

(1) Interrupting attack. Because the GSU packets are sent by broadcasting, the attacker can not interrupt all routes.

(2) Juggling attack. The packets have summary. If the packets are changed by illegal nodes, the summary will be wrong.

(3) Replaying the old GSU packets. Every packet sent by the same node has a different sequence, other nodes will store the sequence in their local neighbor

information table. If the sequence is not more than the old one, the packet will be dropped.

(4) Forging attack. Every node must be authenticated by other nodes following the three steps in section 3.2. The vicious node can't get the certification of CA (Certificate Authority), so it will be isolated.

(5) Denial of Service (DoS) attacks. In order to guarantee the responsiveness of the routing protocol, nodes maintain a priority of their neighbors when detecting neighbors. If some nodes send their packets in high frequency, SGSR will reduce their priority. So if malicious nodes broadcast requests at a very high rate, they will be throttled back.

5 Formal Analysis

SGSR's security is based on the assumption that "only the legitimate node can get the key and certificate from authority". So the malicious node can't get the key and certificate, then it can't generate the validate signature which means it can't generate false Topology Message or alter other's routing packets undetectably. And at the same time he also can't pass the identity authentication.

There are two ways for nodes to get its certificates. One is by the certificate authority [8]. We can define one or more certificate authorities (CA) to take charge of signing the legitimate node's certificate. The other is by transitive trust and PGP trust graphs [9]. In this way, each node signs certificates for other nodes. A node can search in the network to find a chain of certificates beginning at the node initiating the query and ending at the node trying to authenticate a message. Of course, such schemes require transitive trust.

Next we present a formal analysis of the identity authentication process and verify that the goals are achieved. The analysis follows the methodology of BAN logic [10]. We follow the notation and inference rules in [11]. The Appendix provides a detail of the notations.

5.1 Initialization Assumption

$$A \models \xrightarrow{K_{CA}} CA \ , \ B \models \xrightarrow{K_{CA}} CA \ , \ A \models \#(Na) \ , \ B \models \#(Na) \ , \ A \models \phi(\{\xrightarrow{K_B} B\}_{K_{CA}^{-1}}) \ ,$$

$$A \models \#(\{\xrightarrow{K_B} B\}_{K_{CA}^{-1}}) \ , \ B \ni KCA \quad B \models \phi(\{\xrightarrow{K_A} A\}_{K_{CA}^{-1}}) \ , \ B \models \#(\{\xrightarrow{K_A} A\}_{K_{CA}^{-1}}) \ ,$$

$$A \ni KCA \ , A \models \xrightarrow{KA} A \ , \quad B \models \xrightarrow{KB} B \ , \quad A \models \#(KTC\_A) \ , A \models \#(KTC\_B) \ ,$$

$$B \models \#(KTC\_A) \ , \quad B \models \#(KTC\_B) \ , B \models CA \models\Rightarrow \xrightarrow{K_A} A \ , \quad A \models CA \models\Rightarrow \xrightarrow{K_B} B$$

5.2 Protocol Idealization

The purpose of the identity authentication is that after three messages exchanged A will believe the message 2's signature is correct and come from B and B believes the signature of message 3 is correct and come from A. In a word, the aims are

$A \models B \ni KTC\_B, B \models A \ni KTC\_A, A \models B \ni K_B^{-1}, B \models A \ni K_A^{-1}$

The three processes are as follow:

(1) $A \rightarrow B : \{\xrightarrow{K_A} A\}_{K_{CA}^{-1}}, \{N_a\}_{K_A^{-1}}$

(2) $\mathrm{B} \rightarrow A : \{KTC\_B, Na+1\}_{K_B^{-1}}, \{\xrightarrow{K_B} B\}_{K_{CA}^{-1}}$

(3) $A \rightarrow B : \{KTC\_A, Na+2\}_{K_A^{-1}}$

5.3 Logical Postulates

(1) Being-Told Rules: $\dfrac{P \lhd (X,Y)}{P \lhd X, P \lhd Y}$

(2) Possession Rules: $\dfrac{P \ni X, P \ni Y}{P \ni (X,Y)}$

(3) Freshness Rules: $\dfrac{P \models \#(X)}{P \models \#(X,Y), P \models \#(F(X))}$

(4) Recognizability Rules: $\dfrac{P \models \phi(X)}{P \models \phi(X,Y), P \models \phi(F(X))}$

(5) Message Interpretation Rules:

$$\frac{P \models Q \mid\sim X, P \models \#(X)}{P \models Q \ni X}$$

5.4 Analysis

(1) Now from recognizability rules, we can obtain: $\dfrac{B \models \phi(\{\xrightarrow{K_A} A\}_{K_{CA}^{-1}}), B \ni KCA}{B \models \phi(\xrightarrow{K_A} A)}$

B receives Message 1 and gets $\dfrac{B \lhd \{\xrightarrow{K_A} A\}_{K_{CA}^{-1}}, B \ni KCA, B \models \phi(\xrightarrow{K_A} A)}{B \models CA \mid\sim (\phi \xrightarrow{K_A} A)}$

Use the freshness rules: $\dfrac{B \models \#(\{\xrightarrow{K_A} A\}_{K_{CA}^{-1}}), B \ni KCA}{B \models \#(\xrightarrow{K_A} A)}$

From the two previous results, we get: $\dfrac{B \models CA \mid\sim \xrightarrow{K_A} A, B \models \#(\xrightarrow{K_A} A)}{B \models CA \models \xrightarrow{K_A} A}$

Now using the jurisdiction rules, we get: $\dfrac{B \models CA \mid\Rightarrow \xrightarrow{K_A} A, B \models CA \models \xrightarrow{K_A} A}{B \models \xrightarrow{K_A} A}$

which means B believes K_A is public key of A.

(2) When A receives the message 2, similarly A can get $A \models \xrightarrow{K_B} B$

also A will can see $\dfrac{B \lhd \{KTC\_B, Na+1\}_{K_B^{-1}}, A \models \xrightarrow{K_B} B)}{A \models B \mid\sim \{KTC\_B, Na+1\}}$

Use the freshness rules: $\dfrac{A \models \#(Na)}{A \models \#(KTC\_B, Na+1)}$

Use the Message Interpretation Rules

$$\frac{A \models B \mid\sim \{KTC\_B, Na+1\}, A \models \#(KTC\_B, Na+1)}{A \models B \ni \{KTC\_B, Na+1\}}$$

$$\frac{A \lhd \{KTC\_B, Na+1\}_{K_B^{-1}}, A \models \xrightarrow{K_B} B, A \models \phi(KTC\_B, Na+1), A \models \#(KTC\_B, Na+1)}{A \models B \ni K_B^{-1}}$$

so we can say $A \models B \ni KTC\_B$, $A \models B \ni K_B^{-1}$

(3) Similarly B can get: $B \models A \ni KTC\_A$, $B \models A \ni K_A^{-1}$.

At last, we get the aim $A \models B \ni KTC\_B, B \models A \ni KTC\_A, A \models B \ni K_B^{-1}, B \models A \ni K_A^{-1}$

6 Simulation Comparison

To compare the performance between SGSR and LSR, we used GloMoSim to simulate the two routing protocols. GloMoSim is developed by UCLA to simulate the wireless network routing protocol.

The settings of environmental and systemic variable are as follows: The area is 3000 x 3000 m^2, the average speed of the nodes is alterable and the number of the nodes and the connections of the nodes are alterable.

Fig.3 shows the comparison in consumption of energy between SGSR and LSR. The consumption of the energy doesn't increase notablely in proportion to the number of nodes.

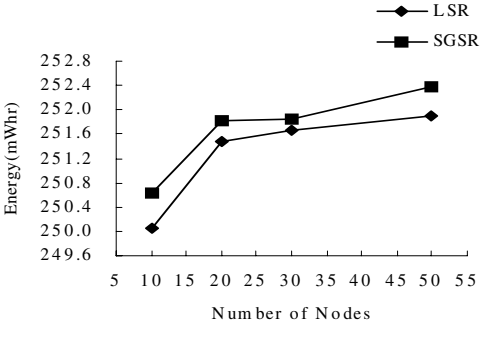


Fig. 3. Consumption of energy

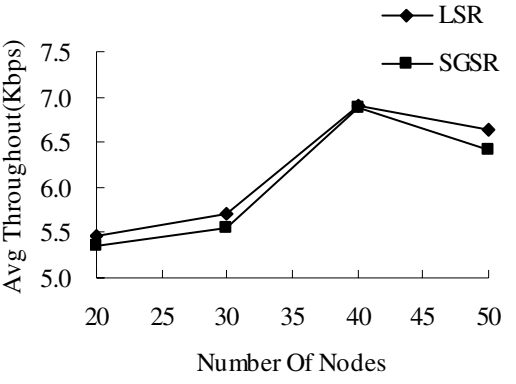


Fig. 4. Average throughput of network in the same rate of the connections

Fig.4 shows that the situation of the throughput with nodes increases when the total network load ratio(the number of connections / the number of nodes in CBR) is changeless. The average throughput rises first and descend later. The reason is that, the throughput will rise with the nodes adding, but when the nodes became more and more dense, the collision will be more and more. The average throughput descends with the collision adding.

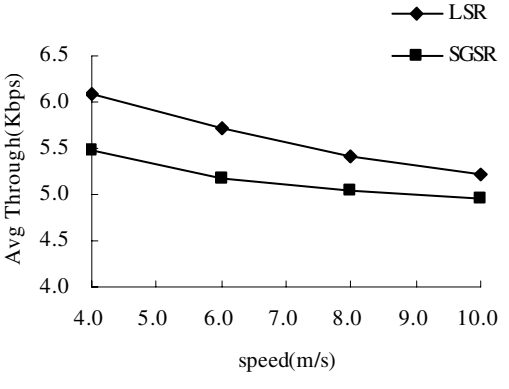


Fig. 5. Average throughput of 50 nodes with increasing speed

Fig.5 shows that when the number of nodes is fixed, the average throughput descends with the nodes' movement rate increasing. The throughput of SGSR is smaller than that of LSR, because with the nodes moving more and more quickly, lose packets rate and collision rate will became bigger and bigger. SGSR adds some fields for authentication or hash link. With the packets' length increasing, the collision will be more serious and the average throughput will descend.

As the three pictures show, the efficiency and the cost of the protocol are in an acceptable scope with adding the security mechanisms.

7 Conclusions and Future Work

We proposed a Secure Global State Routing Protocol (SGSR) for mobile ad hoc networks. SGSR for mobile ad hoc networks strengthens the security of LSR. The securing of the locally proactive topology discovery process by SGSR can be beneficial for MANET for a number of reasons. The security mechanisms of SGSR can adapt to a wide range of network conditions, and thus retain robustness along with efficiency.

As the next step of our research, we will present a detailed performance evaluation of SGSR, both independently and as part of a hybrid framework (i.e., combine it with a secure reactive protocol), and for various network instances and node processing capabilities.

References

[1] Robertazzi.T.G,Sarachik. Self-organizing communication network[j].IEEE ommunmag, 1986, 2~ 5.

[2] Y-C. Hu, A. Perrig, D. B. Johnson. "Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks." *MobiCom '02*, Sept. 23-26, Atlanta, GA.

[3] G. Pei, M. Gerla, and T.-W. Chen, "Fisheye State Routing in Mobile Ad Hoc Networks", Proceedings of Workshop on Wireless Networks and Mobile Computing, Taipei, Taiwan, Apr. 2000, 1~ 3.

[4] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang. "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks." IEEE ICNP 2001, Riverside, CA, Nov. 2001, 5~ 7.

[5] P. Papadimitratos and Z.J. Haas, "Securing the Internet Routing Infrastructure," *IEEE Communications Magazine*, Vol. 40, No. 10, Oct. 2002.

[6] M. G. Zapata, N. Asokan. "Securing Ad hoc Routing Protocols." *1st ACM WiSe*, Atlanta, GA, Sept. 28, 2002.

[7] P. Papadimitratos and Z.J. Haas. "Secure Routing for Mobile Ad Hoc Networks," *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, San Antonio,TX, January 27-31, 2000

[8] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks", *IEEE Network Magazin*e, IEEE Press, vol. 13, no. 6, 1999, pp. 24–30.

[9] S. Capkun, L. Buttyan and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks", *IEEE Transactions On Mobile Computer*, IEEE Press, vol.2, no.1, 2003,pp. 52–63.

[10] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication", *ACM Transactions on Computer System*, vol.8, no. 1, February 1990, pp. 18–36.

[11] L. Gong, R. Needham, and Yahalom, "Reasoning about Belief in Cryptographic Protocols", *Proceeding of the 1990 IEEE Symposium on Research in Security and Privacy,* IEEE Computer Society Press, 1990, pp. 234–248.

[12] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", *Proc. 8th Ann. Int'l Conf. Mobile Computing and Networking* (MobiCom2002), ACM Press, 2002, pp.12–23.

Appendix

X and Y are formulas, P and Q are two principals, C is a statement, K/K^{-1} stand for the principal's public and private key. The basic notations used in section 5 are as follows:

- (X, Y): conjunction of two formulas; it is treated as a set with properties of associativity and commutativity.
- H(X): a one-way function of X. It is required that given X it is computationally feasible to compute H(X); given H(X) it is infeasible to compute X; it is infeasible to compute X and X' such that $X \neq X'$ but $H(X) = H(X')$.

Basic Statements

- $P \triangleleft X$: P is *told* formula X.
- $P \ni X$: P *possesses* or is capable of possessing formula X.
- $P \mid\sim X$: P once conveyed formula X.
- $P \mid\equiv \#(X)$: P *believes*, or is entitled to believe, that formula X is *fresh*. That is X has not been used for the same purpose at any time before the current run of the protocol.
- $P \mid\equiv \phi(X)$: P *believes*, or is entitled to believe, that formula X is *recognizable*. That is, P would *recognize* X if P has certain expectations about the contents of X before actually receiving X. P may recognize a particular value (e.g. his own identifier), a particular structure (e.g. the format of a timestamp), or a particular form of redundancy.
- $P \mid\equiv \xrightarrow{K} Q$: P *believes*, or is entitled to believe, that K is a suitable *public key* for Q. The matching *secret key* K^{-1} will never be discovered by any principals except Q or a principal trusted by Q. In this case, however, the trusted principal should not use it to prove identity or to communicate.
- $P \mid\equiv C$: P *believes* or is entitled to believe that C holds.
- $P \Rightarrow C$: P has *jurisdiction* over statement C.

The *horizontal* line separating two statements or conjunctions of statements signifies that the upper statement *implies* the lower one.

ARSM: Auto Rate Selection Multicast Mechanism for Multi-rate Wireless LANs*

José Villalón, Yongho Seok, Thierry Turletti, Pedro Cuenca, and Luis Orozco-Barbosa

Instituto de Investigación en Informática de Albacete,
Universidad de Castilla-La Mancha, 02071 Albacete, Spain
{josemvillalon, pcuenca, lorozco}@dsi.uclm.es
Institut National de Recherche en Informatique et en Automatique, INRIA
Sophia Antipolis, France
{Yongho.Seok, Thierry.Turletti}@sophia.inria.fr

Abstract. Multicast is an efficient paradigm for transmitting data from a sender to a group of receivers. The IEEE 802.11 wireless LANs standards specify how to send multicast frames with no ACK and using one of the Basic Service Set (BSS) rates. This situation has led many researchers to design techniques aiming to improve reliability of a multicasting mechanism. The Leader-Base Protocol (LBP) is one such mechanism proposed in the literature that is the most promising approach. The main idea behind the design of the LBP mechanism is to reduce the probability of collision of the feedback messages sent by the multicast group members. However, the LBP mechanism falls short by not considering the varying conditions characterizing the wireless channels. In this paper, we introduce a novel auto rate selection multicast mechanism for multi-rate wireless LANs, namely ARSM (Auto Rate Selection for Multicast), capable of adapting the data transmission to the varying conditions of the channel. Our simulation results show that our new scheme outperforms the IEEE 802.11 and the LBP mechanisms.

1 Introduction

The IEEE 802.11 *Media Access Control* (MAC) protocol provides a physical-layer multi-rate capability [1]. The original IEEE 802.11 protocol supports a single base rate, typically 2Mbps. With the multi-rate enhancement, the data transmission can take place at various rates according to the channel conditions. Higher data rates than the base rate are possible when the *Signal-to-Noise Ratio* (SNR) is sufficiently high. Within the IEEE 802.11a standard [2] the set of possible data rates are 6, 9, 12, 18, 24, 36, 48 and 54 Mbps whereas for the IEEE 802.11b standard [3] the set of possible data rates includes 1, 2, 5.5 and 11 Mbps. Since the multi-rate enhancements are

* This work was supported by the Ministry of Science and Education of Spain under CICYT project TIC2003-08154-C06-02, the Council of Science and Education of Castilla-La Mancha under project PAI06-0106, FEDER and the Korea Research Foundation Grant funded by the Korean Government (MOEHRD) (KRF- 2005-214-D00340).

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 239 – 250, 2006.

implemented into the physical layer, the MAC mechanisms should be adapted in order to fully exploit them. The *Auto Rate Fallback* (ARF) protocol is the most known commercial implementation of the IEEE 802.11 MAC making use of this feature [4]. Under the ARF protocol, after the reception of ten consecutive *Acknowledgements* (ACK), the next higher mode is selected for future data frames. If the delivery of the eleventh frame is unsuccessful, it immediately falls back to the previously supported mode. During other cycles with less than ten consecutive ACKs, it switches to a lower rate mode after two successive ACK failures.

Since the ARF protocol selects the data rate taking into account the channel conditions between the *Access Point* (AP) and a given *Mobile Terminal* (MT), it is only suitable for point-to-point communications. In the case of point-to-multipoint communications, i.e., multicast and broadcast services, it is more difficult to determine the highest data rate to be used since the channel conditions between the AP and each one of the MTs in the multicast group may differ and no feedback is available. In most current setups, it comes to the network administrator to setup the data rate to be used by the point-to-multipoint service. This rate is then used to provide network connectivity to all the MTs covered by the AP. It is obvious that in order to ensure full coverage, the rate to be used is determined by using the channel conditions between the AP and the MT exhibiting the worst channel conditions. Furthermore, since the coverage of the AP is inversely proportional to the transmission data rate, the administrator should then select the proper data rate according to the distance between the AP and the worst MT. As the distance increases, the data rate has to be reduced in order to compensate for the increased range that the AP has to cover. This simple approach does not efficiently support the point-to-multipoint communications service.

In this paper, we introduce a novel auto rate selection multicast mechanism for multi-rate wireless LAN, from now on referred as the ARSM mechanism, capable of adapting the data transmission to the varying conditions of the channel. The remainder of this paper is organized as follows. We start Section 2 by providing some background on the issues to be addressed on the design of multicast services to be deployed in a multi-rate wireless LAN. The proposed ARSM mechanism is described in Section 3. Section 4 presents simulation results. Section 5 concludes the paper.

2 Background

In IEEE 802.11 wireless LANs, multicasting is specified as a simple broadcasting mechanism that does not make use of ACK frames. According to the IEEE 802.11a and IEEE 802.11b standards, all frames with multicast and broadcast *Receiver Address* (RA) should be transmitted at one of the rates included in the basic rate set.

Most research efforts on multicasting in IEEE 802.11 wireless LANs have focused on improving transmission reliability by integrating ARQ mechanisms into the protocol architecture. In [5], the *Leader-Based Protocol* (LBP) ARQ mechanism has been proposed to provide the multicast service with some level of reliability. The LBP addresses this issue by assigning the role of group leader to one of the members of the multicast group. The AP designates the MT exhibiting the worst signal quality as group leader. The group leader holds the responsibility to acknowledge the multicast

packets on behalf of all the multicast group members. Any group member other than the leader MT may issue a *Negative Acknowledgement* (NACK) only if it detects an error in the transmission process of the multicast packets addressed to the group. The transmission of the NACK may result in a collision with the ACK issued by the group leader. Upon this event, the sender will once again reissue the multicast frame.

In [6], Gupta et al. present a reliable multicast MAC protocol, namely the 802.11MX protocol. The 802.11 MX uses an ARQ mechanism supplemented by a busy tone signal. When an MT associated to a multicast group receives a corrupted packet, it sends a NACK tone instead of actually transmitting a NACK frame. Upon detecting the NACK tone, the sender will retransmit the data packet. On the contrary, if the AP does not detect the NACK tone, the AP assumes that the transmission of the multicast packet has been successfully completed. Since the 802.11MX mechanism does not need a leader to operate, it performs better than the LBP protocol in terms of both data throughput and reliability. However, this mechanism falls short on addressing events when some of the group members do not properly receive a packet. For instance, in the event that the header of a multicast packet may get corrupted, a group member will be unable to detect it and signal this event.

It should be clear that the mechanisms above described only focus on solving the reliability of the multicast service in wireless LANs. They do not adapt the transmission rate of the multicast packet taking into account the quality of the signal received by each and every member of the multicast group. To the best of our knowledge, there is no related work to provide an auto rate adaptation mechanism for the multicast service over wireless LANs. In this paper, we make use of the multirate capabilities present in the physical layer of the latest IEEE 802.11 wireless LANs for developing a reliable multicast service.

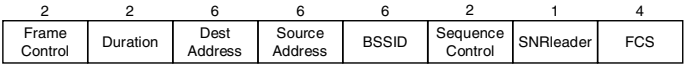
3 Auto Rate Selection for Multicast (ARSM)

The ultimate goal of the ARSM protocol to be introduced herein is to enable the deployment of a reliable and efficient multicast protocol to be integrated into the protocol architecture of multirate wireless networks. By efficient, we mean that the overhead required by the ARSM to operate should be kept to minimum levels. ARSM enables the exchange of information pertaining to the physical channel conditions as perceived by each and every MT. This information can be used by ARSM to determine the transmission rate accordingly. In the following sections, we introduce the various mechanisms making part of ARSM.

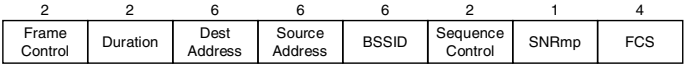
3.1 Multicast Channel Probe Operation (MCPO) of ARSM

ARSM is an adaptive mechanism in which the AP selects the PHY data rate to be used for multicast data transmission. The PHY data rate to be used is determined by taking into account the channel conditions perceived by each and every MT belonging to a given multicast group. Under the proposed scheme, the AP starts by multicasting a control frame, namely the *Multicast Probe* (MP) frame, to the multicast group members. Upon receiving the MP frame, each multicast member estimates the SNR of the channel, i.e., the quality of the wireless medium. Based on the SNR, each MT

will determine the point in time for replying to the AP. According to the proposed mechanism, the MT having detected the lowest SNR will be the one in charge of first replying to the AP, by issuing a *Multicast Response* (MR) frame. Upon detecting the transmission of the reply and in the absence of errors, all the other group members should normally refrain from replying to the AP. The AP then selects the multicast data rate based on the SNR of the reporting MT.



(a) Multicast Probe Frame



(b) Multicast Response Frame

Fig. 1. Special Multicast Control Frames

Figure 1a shows the format of the MP frame. The duration field of the MP frame is initially set to CW_m x *SlotTime*, where CW_m is the length of the contention window, expressed in slots, during which the group members may attempt to transmit the MR frame back to the AP. The destination address field of the MP frame represents the address of the multicast group being addressed by the AP and the SNR_{leader} field is set to the SNR received in the latest acknowledgement received by the AP.

After having sent the MP frame, the AP will wait for a period whose length is given by the *Short Inter Frame Space* (SIFS) parameter of the IEEE 802.11 standard, before changing its interface from transmission mode to listen mode. At the time of sending the multicast frame, the AP starts a timer, namely the *MP_timer,* initially setting to CW_m slots. The timer is then decremented by one slot whenever the channel has been sensed idle for a period of time equal to one time slot (*SlotTime*). On the contrary, whenever the AP detects activity in the channel by means of the *Clear Channel Assessment* (CCA) mechanism, it immediately freezes the *MP_timer*.

When a MT receives the MP frame, it checks whether it is a member of this multicast group. If it is not, it sets the NAV parameter to CW_m x *SlotTime* by using the duration field included in the MP frame. In this way, the MTs that are no members of the multicast group will not interfere with the on-going multicast transmission. Figure 1b depicts the format of the MR frame.

In the MR frame, the SNR_{mp} field contains the SNR value of the previously received MP frame. When a MT replies to the AP with an MR frame, an MT uses the backoff mechanism in order to reduce the collision probability with other MR frames. The backoff timer used for transmitting the MR frame is set according to the following expression:

$$BackoffTimer = \begin{cases} [0,2] & SNR_{mp} < SNR_{leader} - F1 \\ [3,5] & SNR_{leader} - F1 \le SNR_{mp} < SNR_{leader} \\ [6,7] & SNR_{leader} \le SNR_{mp} \end{cases} \quad (1)$$

where *F1* is a correcting factor to limit the SNR intervals. From this expression, it is clear that the backoff timer is chosen based on the channel quality of the MT. The MT with the worst SNR chooses the lowest backoff timer and has a chance to transmit the MR frame earlier than all other MTs. In order to reduce the probability of collision of the MR frames, a random number of slots have been assigned to each one of the three intervals. When all the other MTs detect the transmission of the MR frame, all the other MTs refrain from transmitting. In this way, ARSM avoids the MP frame implosion problem.

Following the multicast channel probe operation, the AP selects the appropriate PHY data rate using the feedback information that contains the channel conditions of the MTs. According to the received information, and the value of the *MP_timer*, the AP could receive three different kinds of feedback information: *Explicit Feedback*, *Implicit Feedback*, *and No Feedback*.

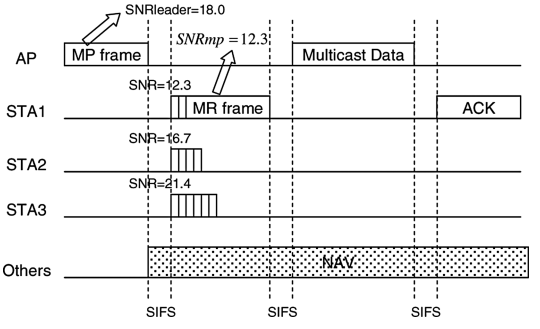


Fig. 2. Explicit Feedback Scenario

Explicit Feedback: the AP receives the MR frame from an MT within the multicast group. In this case, the AP determines the SNR value of the MT with the worst channel quality. Then, it transmits the multicast data frames accordingly. In the scenario depicted in Figure 2, STA1 selects the shortest backoff time since STA1 shows the worst received SNR of MP frame. STA1 then sends the MR frame to the AP after 3 slots; this period is determined through Equation 1.

Implicit Feedback: the AP receives a corrupted MR frame and the MP timer of the AP has not expired. This condition occurs when several MTs reply to the MP frame simultaneously and the MR frames have collided. In this case, the AP can predict an SNR value of MTs with the worst channel quality through the current MP timer value. Through the current MP timer of the AP, the AP identifies the lowest backoff timer among all the MTs in the multicast group. It must be mentioned that the MT with the lowest backoff timer first replies to the AP using an MR frame. The AP should already know the value of the backoff timer chosen by the MT to send MR frame. Using Equation 2, the AP can inversely estimate the SNR range with the lowest backoff timer, where BT_{mp} is the current MP timer value in AP and $\overline{SNR}$ is the estimated worst SNR value.

$$\overline{SNR_{mp}} = \begin{cases} 0 & BT_{mp} \geq 6 \\ SNR_{leader} - F1 & 6 > BT_{mp} \geq 3 \\ SNR_{leader} & 3 > BT_{mp} \geq 1 \end{cases} \quad (2)$$

Figure 3 shows an example of implicit feedback scenario of the ARSM mechanism. The AP does not receive the MR frame because both MTs, STA1 and STA2, simultaneously have sent an MR to the AP. The MR frames will collide before the MP timer of the AP expires. By using the value of the remaining period of the MP timer of the AP, ARSM is able to estimate the lower bound of MT exhibiting the worst SNR. In this scenario, the worst SNR estimated from the MTs ($\overline{SNR}$) is greater than 15dB; the AP then chooses the multicast rate corresponding to 15dB.

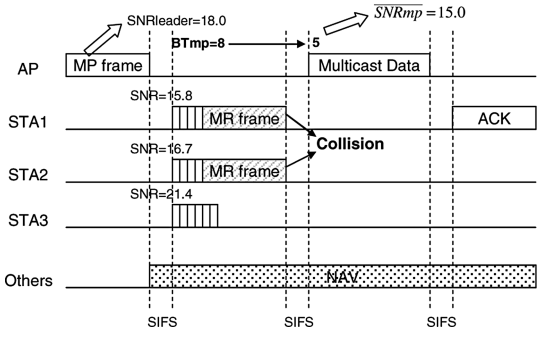


Fig. 3. Implicit Feedback Scenario

No Feedback: The AP does not receive an MR frame and the MP timer of the AP expires. So, none of the MTs in the multicast group reply to the MP frame. This means that either all the MTs in this group have left or that the MP frame has been corrupted during its transmission. In this case, the AP will retransmit the MP frame after waiting for a period of time defined by the DCF backoff mechanism. The number of retransmission attempts for a given MP frame is limited to 4. When the maximum number of retransmission attempts is selected, the AP assumes that there are no more MTs in the multicast group.

The AP then determines the PHY data rate to be used for the multicast data transmission using the CLARA mechanism [7]. With this mechanism, a MT makes use of the SNR of the feedback signal in order to adapt its data rate to the actual channel conditions. The SNR value is obtained by either explicit feedback (SNR_{mp}) or implicit feedback ($\overline{SNR}$).

The AP can determine the MT exhibiting the worst SNR by using a channel probe mechanism in the absence of a collision involving the MR frame (*Explicit Feedback*). However, if the MR frame collides (*Implicit Feedback*), the AP is unable to identify the new leader. In this case, to identify the new leader, the AP will have to send an MP frame before sending the following multicast data frame. The new MP frame to be sent out will set the SNR_{leader} field to a negative value. When the MTs in the multicast group receive the MP frame with the SNR_{leader} field equal to a negative

value, only those MTs having sent the previous MR frame (the MTs with smaller SNR) sent to this a new MR frame. Since these MTs will have a very similar SNR, they do not use the backoff mechanism based on the SNR of the received signal, but a random value between [0, CW_m-1]. This different backoff mechanism is used to further reduce the probability of collision of the MR frames.

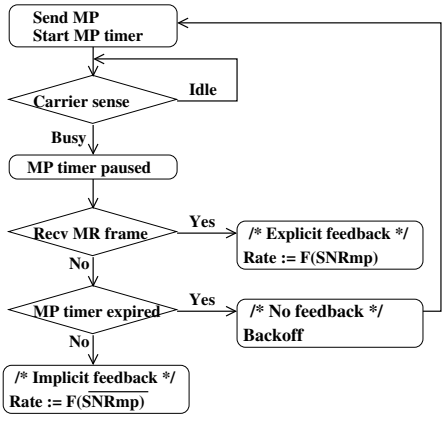


Fig. 4. Multicast Channel Probe Operation (MCPO) of ARSM

Figure 4 shows the MCPO procedure of ARSM. As shown in Figure 4, after having sent an MP frame, the AP will activate its MP timer with the initial value CW_m. The timer will remain active as long as the AP detects that the channel is busy. If the AP receives an error-free MR frame before the timer expires, it will adapt its transmission rate using the explicit feedback. On the contrary, if the AP receives a corrupted MR frame, once its timer expire, the PHY data rate will be selected based on the implicit feedback mechanism.

3.2 Dynamic Multicast Data Transmission Procedure

Through the multicast channel probe operation, the AP can estimate the worst SNR of MTs. In order to reduce the amount of processing to be carried out by the MTs, we propose a dynamic multicast data transmission procedure by making use of several multicast data transmissions. Under this scheme, the AP can be found in one of two different states depending on the feedback signals received.

- While the AP successfully delivers multicast data frame, the *Multicast Channel Probe Operation* is deactivated. In this state, the AP will adapt its PHY data rate using the SNR value contained in the received ACK coming from the group leader using the CLARA mechanism.
- If the AP shows a failure of N_{th} consecutive multicast transmissions, it initiates the *Multicast Channel Probe Operation*.

However, this dynamic multicast data transmission needs a mechanism for determining whether the multicast packet has been successfully delivered or not. The IEEE 802.11 standard does not support any mechanism to carry out this verification

for the multicast service. On this purpose, we use the LBP mechanism. By combining the LBP and CLARA mechanisms, the ARSM mechanism can adapt the data rate taking into account the SNR included in the ACK received from the group leader.

Figure 5 shows an example of the operation of the ARSM mechanism. The mechanism starts by using the MCPO in order to determine the multicast group leader. In this example, the group leader becomes STA1 which is the MT with the lowest SNR value. The AP then turns off the MCPO and starts sending the data frames. After two successful transmissions, it is assumed that STA2 becomes the MT with the worst SNR. This happens at 35 ms of operation. Since the AP has not become aware of the SNR change of STA2, the AP continues sending the data frames at the same data rate. After the N_{th} transmission failure, the AP turns on the multicast channel probe operation. With the explicit feedback information from STA3, the AP sets STA3 as the group leader. This happens at 60 ms of operation.

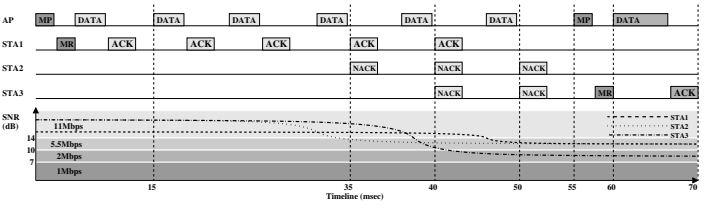


Fig. 5. Dynamic Multicast Data Transmission Procedure

4 Performance Evaluation

In this section, we carry out a performance analysis on the effectiveness of our proposed mechanism. Throughout our study, we have made use of the OPNET Modeler tool 11.0 [8], which already integrates the IEEE 802.11 DCF simulator. We have integrated into it the ASRM and the LBP mechanisms.

4.1 Scenarios and Metrics

Our performance evaluation has been structured in the following way: first we analyze the performance limitations of the multicast service of the IEEE 802.11 standard. We then evaluate and compare the ARSM and LBP schemes. Towards this end, we have studied the performance of the two schemes by varying the size of the network (coverage area) and using two different multicast group sizes.

In our simulations, we model an IEEE 802.11b WLAN consisting of an AP, several multicast wireless MTs, and five unicast wireless MTs. All MTs are located within a *Basic Service Set* (BSS), i.e., every MT is able to detect a transmission from any other MT. The access point is located in the center of the BSS, which cell size will be changed throughout the different scenarios under study. The multicast MTs move randomly within the BSS with a constant speed of 5 km/h, whereas the unicast MTs are static and placed close to the access point. We assume that the unicast packets are always transmitted at 11 Mbps. This setup of the unicast MTs will allow

us to focus on the evaluation of each one of the multicast schemes under consideration.

For the ARSM scheme, we have set $F1 = 3$ and $n_{th} = 3$. These values have been determined after an extensive campaign of simulations. By setting $F1 = 3$, the number of collisions of the MR frame is considerable reduced. This value corresponds to the distance between the thresholds being used to adapt the transmission rate taking into account the state of the channel. In the case of the value used for n_{th}, we have come to a compromise to limit the number of MP frames to be sent and the time to react to a change on the network. In the case of the *CW* parameter, we have set it to 8. This value is fully compliant to the standard and corresponds to the length of the Extended IFS (EIFS) parameter of the IEEE 802.11 standard.

In order to model the wireless channel, we have used the *Ricean* model to characterize the propagation of the signal throughout the medium [9]. When there is a dominant stationary signal component present, such as a line-of-sight propagation path, the small-scale fading envelope has a Ricean distribution. This is often described in terms of a parameter k, which is defined as the ratio between the deterministic signal power and the variance of multi-path fading. If k is equal to 0, the Ricean distribution reduces to the Rayleigh distribution, in which the signal is only transmitted by reflection. In this work, we have set the parameter k to 32.

In our scenarios, we have assumed the use of two types of traffic flows: multicast traffic downlink flows and unicast traffic uplink flows. For the downlink traffic, the access point transmits a video stream to the multicast MTs group. For the video streaming source, we have used traces generated from a variable bit-rate H.264 video encoder [10]. We have used the sequence *Mobile Calendar* encoded on CIF format at a video frame rate of 25 frames/s. The average video transmission rate is around 400 Kbits/s with a packet size equal to 1000 bytes (including RTP/UDP/IP headers). This video application is randomly activated within the interval [1,1.5] seconds from the start of the simulation. In order to limit the delay experienced by the video streaming application, the maximum time that a video packet may remain in the transmission buffer has been set to 2 seconds. Whenever a video packet exceeds these upper bounds, it is dropped. For the unicast traffic, we assume greedy sources. The unicast packet size is equal to 1000 bytes (including the RTP/UDP/IP headers). The unicast sources are also randomly activated within the interval [1,1.5] seconds from the start of the simulation. Throughout our study, we have simulated the two minutes of operation of each particular scenario.

In our simulations, we have started by simulating a WLAN consisting of five unicast MTs and nine multicast MTs. The network size has been initially set to a geographical area of 50m x 50m. We have then increased the network size in both dimensions by 10m x 10m to a maximum network size of 140m x 140m. Then, the size for the multicast group has been increased to 18 MTs.

For the purpose of our performance study, the three metrics of interest are: *multicast throughput*, *unicast throughput*, and *multicast packet loss rate*. The multicast throughput shows the successfully received average data rate by all the multicast MTs. To be able to better evaluate the various schemes with respect to the optimum case, we plot the normalized throughput rather than the absolute throughput. The normalized throughput is calculated with respect to the multicast downlink traffic generated by the AP. The unicast throughput shows the total throughput received by

the AP from all the unicast MTs. This metric will allow us to estimate the bandwidth not used (available for unicast sources) of each one of the multicast schemes under consideration. Finally the multicast packet loss rate shows the ratio between the packets not having been received by at least a member MT of the multicast group over the total number of packets submitted to the network.

Our measurements started after a warm-up period (about three seconds) allowing us to collect the statistics under steady-state conditions. Each point in our plots is an average over thirty simulation runs, and the error bars indicate 95% confidence interval.

4.2 Results

In the first part of our performance study, we first look at the multicast service as defined by the standard. We have first considered a small-sized network; this setup represents the most manageable of all setups being considered, i.e., the potential number of corrupted packets is limited. Figure 6 shows the results for this first scenario. From the results, it is clear that the standard is unable to effectively provide multicast services. This is due to the fact that the standard does not take any action to recover those packets having been corrupted or lost during their transmission. A loss rate of 18% is far below all expectations, especially if we do consider the deployment of video streaming applications.

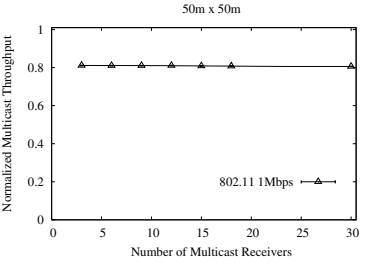


Fig. 6. Limitations IEEE 802.11 Standard for the Multicast Traffic

Figure 7 shows the multicast throughput obtained for both schemes under study. The results depicted in Figure 7 show that ARSM and LBP (1Mbps) schemes are able to provide a reliable multicast for all network sizes. For all the other rates, the performance of LBP decreases as the network size is increased. This is expected since adapting the transmission helps to compensate for the signal impairments due to the distance to be covered by the signal. The figure 7b shows the effect to increase the size of multicast group. This figure shows that the performance of LBP mechanisms decreases more quickly when the size of the multicast group is increased.

For the case of the unicast traffic, figure 8 shows that the ARSM outperforms the LBP 1Mbps for all network sizes. Furthermore, in the case of small-sized network, ARSM is even able to deliver twice the load carried by the LBP 1Mbps scheme. The figure also shows that the ARSM outperforms the LBP scheme when this latter is able to fully deliver the multicast traffic (see figure 7). The results clearly show the benefits of adapting the transmission rate taking into account the channel conditions.

The figure 8b shows the effect to increase the number of multicast receivers. The results in this figure show that the ARSM scheme is able to cope with large multicast group sizes.

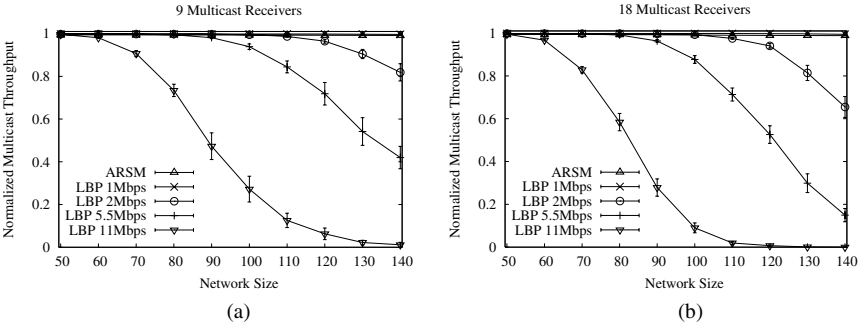


Fig. 7. Throughput of Multicast Traffic: a) 9 Multicast receivers, b) 18 Multicast receivers

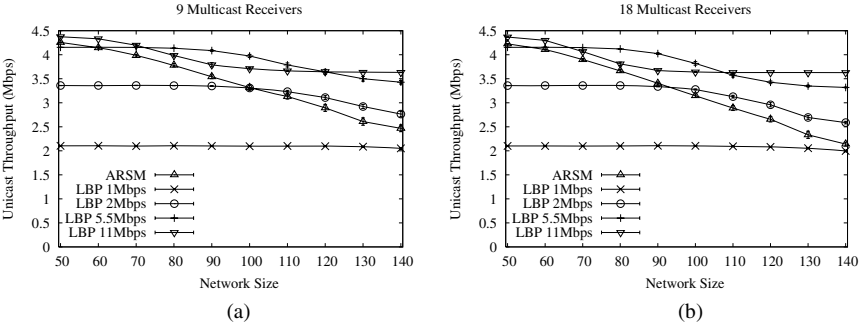


Fig. 8. Total Throughput of Unicast Traffic: a) 9 Multicast receivers, b) 18 Multicast receivers

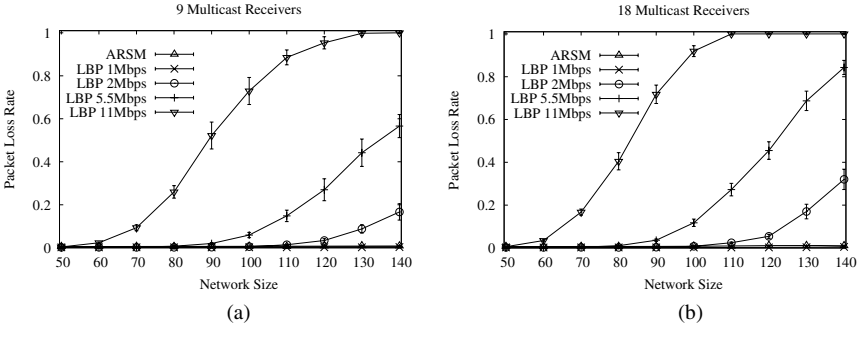


Fig. 9. Packet Loss Rate of Multicast Traffic: a) 9 Multicast receivers, b) 18 Multicast receivers

Finally, figure 9 shows the multicast packet loss rate for the ARSM and LBP schemes. This figure shows clearly how the LBP scheme is unable to provide good support to the multicast service for all the network sizes even at rates as low as 2Mbps. The figure shows that only ARSM and LBP 1Mbps schemes are able to provide a reliable multicast for all network sizes.

5 Conclusions

We have proposed an adaptive IEEE 802.11 multicast protocol design that takes into account the dynamic channel conditions. The mechanism requires knowing the operating conditions of the channel as perceived by the multicast group members. The transmission rate to be used for the multicast traffic is determined based on the feedback received by the group leader. We have also paid particular attention to limit the overhead introduced by the multicast rate adaptation mechanism. We have carried out an extensive campaign of simulations aiming to analyze the impact of various key parameters, mainly the network size and the size of the multicast group, over the performance of the proposed scheme. Our results have shown that the ARSM mechanism outperforms the IEEE 802.11 and LBP mechanisms.

References

1. LAN MAN Standards Committee of the IEEE Computer Society, ANSI/IEEE Std 802.11, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999 Edition.
2. LAN MAN Standards Committee of the IEEE Computer Society, ANSI/IEEE Std 802.11, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5GHz Band", IEEE 802.11 Standard, 1999.
3. LAN MAN Standards Committee of the IEEE Computer Society, ANSI/IEEE Std 802.11, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer Extension in the 2.4 GHz Band", IEEE 802.11 Standard, 1999.
4. A. Kamerman, and L. Monteban, "WaveLAN II: A High-Performance Wireless LAN for the Unlicensed Band", Bell Labs Technical Journal, page 118-133, Summer 1997.
5. Joy Kuri and Sneha Kumar Kasera, "Reliable Multicast in Multi-access Wireless LANs", ACM Wireless Networks, Volume 7, Issue 4, Pages 359 - 369, 2001.
6. S. K. S. Gupta, V. Shankar and S. Lalwani, "Reliable Multicast MAC Protocol for Wireless LANs", IEEE ICC, May 2003.
7. C. Hoffmann, M. H. Manshaei and Thierry Turletti, "CLARA: Closed-Loop Adaptive Rate Allocation for IEEE Wireless LANs", IEEE WIRELESSCOM, June 2005.
8. Opnet.Technologies.Inc. OPNET Modeler 10.0 (c)1987-2004. http://www.opnet.com.
9. Ratish J. Punnoose, Pavel V. Nikitin, and D. Stancil, "Efficient Simulation of Ricean Fading within a Packet Simulator", IEEE Vehicular Technology Conference, 2000.
10. ITU-T Recommendation H.264, "Advanced Video Coding For Generic Audiovisual Services". May 2003.

On Self-coordination in Wireless Community Networks

Frank A. Zdarsky, Ivan Martinovic, and Jens B. Schmitt

disco | Distributed Computer Systems Lab
University of Kaiserslautern, 67655 Kaiserslautern, Germany
{zdarsky, martinovic, jschmitt}@informatik.uni-kl.de

Abstract. Co-channel interference and contention at shared medium access may significantly degrade the performance of a CSMA/CA-based wireless LAN. While this phenomenon may be controlled within a single administrative domain by choosing appropriate access point installation sites and assigning operating channels intelligently, there is little that can be done against interference by access points from other nearby administrative domains. This problem becomes paramount in so-called *wireless community networks*, as each access point is operated by a different owner and can be viewed as a separate domain. In this paper we propose a *distributed algorithm and protocol for self-coordination of access points* from different domains based solely on knowledge about the immediate neighborhood. We show that our distributed coordination algorithm may lower contention by around 19% compared to standard WLAN.

Keywords: Wireless LANs, contention, self-coordination.

1 Introduction and Motivation

The emergence of wireless community networks (e.g. NYCwireless[1]) is a remarkable and growing phenomenon that is fueled by the desire of ubiquitous, low-cost, and high-speed Internet access. These networks are based on access points which are independently run by volunteers with their own equipment. The common goal is to enable sharing of wireless Internet access with other members of the community, gradually growing the network to a large, city-wide scale.

Wireless community networks tend to be quite different from the typical wireless LAN deployment. A single public or private organisation is able to preplan access point locations, relying on expert knowledge or using commercially available WLAN planning tools. As a result, these networks may cover an area with comparatively few access points and little overlap between co-channel radio "cells". In contrast, wireless community networks usually grow in an unplanned, evolutionary process, and their access point locations are defined by the users willing to participate. Some areas covered by such networks may therefore have very high node densities. In fact, as observed in [2], areas with densities of more than 10 (and even up to 80!) overlapping access points from different networks are not uncommon in some major U.S. cities. As the number of available non-overlapping channels in IEEE 802.11 WLANs is very low, it is not surprising that the performance in such environments may be severely impaired.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 251–262, 2006.

A solution to this problem is to introduce coordination mechanisms between access points of different administrative domains. While products such as wireless switches[3] and self-configuring access points[4] are available for radio management inside single administrative domains, the problem of inter-domain contention has only recently started to attract the attention of the scientific community[5].

In previous work we have proposed a mathematical model of the minimum inter-domain contention problem and methods for finding near-optimal solutions based on global knowledge[6]. In this paper, we present a distributed algorithm and protocol for the self-coordination of access points that uses only regional knowledge and therefore lends more naturally to the problem of self-coordinating access points from a large number of different administrative domains, as is the case in wireless community networks. We show by simulation that our algorithm may reduce contention by 20% compared to standard WLAN. Furthermore, we show that in dense deployments with only few available channels, the intuitive and frequently proposed approach to load-balance between available access points may *not* be optimal and that it may sometimes be preferable to even *switch off* some access points.

2 Related Work

While the contributions on planning mobile telecommunication networks are numerous, they are only partly transferable to wireless LANs, which employ shared medium access schemes such as CSMA/CA. Comparatively few contributions consider the effects of contention that results from these access schemes.

Network planning problems specific to wireless LANs have been formulated for solving the access point placement problem[7] and the channel assignment problem[8]. Joint placement and channel assignment has been proposed, where co-channel overlapping may be allowed[9] or not[10]. In contrast to these contributions on the *planning* of wireless LANs, in [6] we proposed a model for the case where access point locations are already given and the problem is to determine the configuration of transmission power, channel assignment and associations of stations to access points that will minimize contention in the given network.

Previous work on the online reconfiguration of access points mainly focuses on transmit power control and load sharing in single administrative domains [11,12]. [5] suggest the use of a radio resource broker that controls contention between domains by assigning the channels and transmission powers that each domain may use. While being the most closely related work to ours, this proposal relies on a central component assuming a rather low number of different domains, i.e. it is not suited for a wireless community network.

3 Modeling of the Minimal Contention Problem

In this section we provide a very brief overview of our mathematical programming formulation of the minimal contention problem for CSMA/CA-based

wireless networks. The optimization model takes as parameters the locations and radio configurations of a set of access points (APs) and stations (STAs), and a matrix of propagation losses between each pair of wireless nodes. The model is agnostic of the radio propagation model, so any analytical or empirical model may be used to instantiate the loss matrix. The model allows to determine the configuration of transmission power, channel assignment, and station association that will minimize the amount of contention in a scenario both for basic CSMA/CA and RTS/CTS modes. Due to space restrictions, we have to refer the reader to [6] for details on the model and some of its useful further extensions.

Let i denote a wireless node with $i = 1, \ldots, I + K$, where I is the number of APs in the scenario and K the number of STAs. Nodes shall be ordered such that $i = 1, \ldots, I$ for APs and $i = I + 1, \ldots, I + K$ for STAs. Each node i can transmit with a transmission power $x_i \in [0, ..., s_i]$, where s_i is the maximum allowed power of node i and $x_i \in \mathbb{R}$. On the way from a sender i to a receiver m, a signal experiences a path loss given by p_{im}[1]. A receiving node requires a minimum signal strength r_m to be able to decode a frame transmitted at the desired data rate correctly. If a node i receives a signal from another node with a power above or equal to l_i, its CCA will report the channel as busy.

APs and their associated STAs form basic service sets (BSS). A BSS can operate on one of J different non-overlapping radio channels, $j = 1, \ldots, J$. y_{ij} is a binary variable indicating whether node i currently uses channel j or not. We further define a binary variable f_{im} indicating whether a node i (which must be a STA) is currently associated to node m (an AP) and a helper variable e^{pc}_{im} which indicates whether node i is a potential contender of node m. With potential contender we mean that node m is close enough to i that it can detect i's carrier if both are operating on the same channel.

A valid solution of our optimization problem needs to satisfy several constraints. First of all, each node's transmission power must be between zero and the node-specific maximum:

$$0 \leq x_i \leq s_i, \quad i = 1, \ldots, I + K \tag{1}$$

All STAs have to receive their minimum power requirement from the AP they are associated to:

$$x_i + p_{im} \geq f_{im} r_m, \quad i = 1, \ldots, I,\ m = I + 1, \ldots, I + K \tag{2}$$

Likewise, all APs have to receive their minimum power requirement from the STAs in their BSS:

$$x_m + p_{mi} \geq f_{im} r_i, \quad i = 1, \ldots, I,\ m = I + 1, \ldots, I + K \tag{3}$$

[1] Note that we assume dBm as the unit of signal strength. Due to its logarithmic scale, losses (negative values) in dB are actually added to the transmission power to calculate the received signal strength.

All STAs are associated to exactly one AP:

$$\sum_{i=1}^{I} f_{im} = 1, \quad m = I+1, \ldots, I+K \tag{4}$$

Each AP and STA uses exactly one channel:

$$\sum_{j=1}^{J} y_{ij} = 1, \quad i = 1, \ldots, I+K \tag{5}$$

All STAs use the channel of the AP which they are associated to:

$$y_{ij} - y_{mj} - (1 - f_{im}) \leq 0, \tag{6}$$
$$i = 1, \ldots, I,\ m = I+1, \ldots, I+K,\ J = 1, \ldots, J$$

Finally, we force e_{im}^{pc} to be 1 if nodes i and m are so close to each other, that m detects the channel busy if i currently transmits on the same channel (for $i \neq m$, of course, since nodes cannot contend for access with themselves):

$$x_i + p_{im} \leq l_m + e_{im}^{pc} M_{im}, \quad M_{im} = s_i + p_{im} - l_m \tag{7}$$
$$i = 1, \ldots I+K,\ m = 1, \ldots, I+K \ \wedge \ i \neq m$$

$$e_{ii}^{pc} = 0, \quad i = 1, \ldots, I+K \tag{8}$$

Considering that a node can only contend for access with another node when both are on the same channel, we are able to calculate a_m, the number of nodes contending for access with node m:

$$a_m = \sum_{i=1}^{I+K} e_{im}^{pc} \left(\sum_{j=1}^{J} y_{ij} y_{mj} \right) \tag{9}$$

The objective function that minimizes contention in a CSMA/CA network in basic mode (i.e. without RTS/CTS) can then be stated as:

$$\min \sum_{m=1}^{I+K} a_m = \min \sum_{m=1}^{I+K} \sum_{i=1}^{I+K} e_{im}^{pc} \left(\sum_{j=1}^{J} y_{ij} y_{mj} \right) \tag{10}$$

For a CSMA/CA network in RTS/CTS mode, we furthermore have to take into consideration the indirect contention between wireless nodes. We call a node i an indirect contender of m, if there exists at least one node k that can hear i's RTS frames and whose CTS replies m can hear. In order not to count a node twice, we further require an indirect contender not to be a direct contender at the same time. To indicate that a node is *not* potential direct contender of another node, we need to define a new helper decision variable e_{im}^{npc}:

$$x_i + p_{im} \geq l_m - e_{im}^{npc} M_{im}, \quad M_{im} = l_m - p_{im} \tag{11}$$
$$i = 1, \ldots I+K,\ m = 1, \ldots, I+K \ \wedge \ i \neq m$$

$$e_{ii}^{npc} = 1, \quad i = 1, \ldots, I + K \tag{12}$$

We can now extend $a_m$with the number of indirect contenders, but have to take into consideration that APs only send to STAs but not to other APs and vice versa. Furthermore, an AP that does not have STAs assigned should not be counted as an indirect contender. On the other hand, if it has STAs, it should be counted exactly once, no matter how many STAs are assigned to it. This is why we introduce the step function $\sigma(x)$ with $\sigma(x) = 1$ if $x > 0$ and 0 otherwise. Our objective function thus becomes:

$$\min \sum_{m=1}^{I+K} a_m,$$

$$a_m = \sum_{i=1}^{I+K} e_{im}^{pc} \left(\sum_{j=1}^{J} y_{ij} y_{mj} \right) + \sum_{k=I+1}^{I+K} \sum_{i=1}^{I} f_{ik} e_{ki}^{pc} e_{im}^{pc} e_{km}^{npc} \left(\sum_{j=1}^{J} y_{ij} y_{kj} y_{mj} \right) + \sum_{i=1}^{I} \sigma \left(\sum_{k=I+1}^{I+K} f_{ik} e_{ik}^{pc} e_{km}^{pc} e_{im}^{npc} \left(\sum_{j=1}^{J} y_{ij} y_{kj} y_{mj} \right) \right) \tag{13}$$

The polynomial structure of the presented optimization model make this problem difficult to solve exactly. We have, however, been able to transform this problem into an equivalent linear formulation, which allows us to solve small problem instances with any mixed integer program solver. Due to space restrictions we again refer the reader to [6] for further details. In the same paper we also describe a genetic algorithm heuristic which due to its custom tailored design allows to find near-optimal solutions for comparatively large scenarios (s.a. 200 APs and 400 STAs).

4 Distributed Coordination Algorithm

In this section we describe our distributed algorithm for reducing the contention in a wireless access network. It consists of five building blocks:

- Data dissemination, in which each AP gains knowledge about other APs within its horizon as well as the STAs which these APs are aware of and are able to cover at the required signal strength.
- Local negotiation, in which an AP suggests a local reconfiguration of the network to all APs within its horizon, waits for their feedback on how this reconfiguration would affect network performance in their vicinity and then decides either to commit or abandon this reconfiguration.
- A fitness function with which to evaluate the current state of the network within an APs horizon and the effect of a proposed reconfiguration.
- An algorithm used to find local reconfigurations.

– A mechanism to determine, which APs are allowed to propose local reconfigurations and when.

An AP's *horizon* defines which other APs and STAs in its geographical vicinity it knows and considers in finding improvements. When choosing the extent of the horizon, one has to make the typical trade-off between the chances for finding the globally optimal configuration and the computational effort and signaling overhead. In our experiments we have defined the horizon of an AP i as the set of all APs that are either within contention range of AP i themselves or are able to serve a STA that is in contention range of i.

4.1 Data Dissemination

APs initially find out about their neighbors by scanning for periodic beacon signals on all available channels. Upon receiving a beacon from a previously unknown neighbor, the AP sends out a WELCOME message to its new neighbor, both on the wireless link and on the wired backbone network. This assumes that the IP address of the new neighbor is known. The most simple solution is to let each AP include its IP address as an additional Management Frame Information Element in its broadcasted beacons.

Both the WELCOME message and the reply to it (WELCOME_ACK) contain information about the sending AP and about all STAs which the sender is currently aware of and whose minimum signal strength requirements it can meet. By sending these messages over both the wireless link and the backbone, we can further gain information about whether the wireless link is asymmetric or not, i.e. if one access point is able to hear the other but not vice versa.

Furthermore, all active APs periodically send UPDATE messages to all APs within their horizon containing their current STA information list. This information has an explicit expiration time, so if an AP does not receive UPDATE messages from a neighbor for a certain length of time, it will assume it has deactivated without signing off. UPDATE messages are always sent via the wired backbone, so that this soft-state approach does not consume valuable wireless resources.

We also consider the case that two APs that cannot hear each other directly nevertheless produce contention in each other's BSS. This may happen when an STA is located in between the AP it is associated to and another AP that is within contention range. The STA may then notify its own AP of the contending AP's presence so that both APs may contact each other using the mechanism described above.

4.2 Local Negotiation

Based on its knowledge about APs and STAs within its horizon, an AP may run a local optimization algorithm to search for better configurations for itself and its neighboring APs. If an AP finds a configuration that will improve contention within its own horizon, it suggests the new configuration to its neighbors by sending them an OFFER message with the new configuration.

Upon receiving an OFFER, every neighbor determines the effect of the configuration change on their part of the network. Note that the sets of nodes within the horizons of the APs sending the OFFER and receiving the offer will usually not be identical, although the intersection set should usually be large. All receivers of an OFFER then answer with an OFFER_REPLY message containing the change in contention that would result from actually committing the configuration change. If the net effect of the reconfiguration proposal is positive, the initiating AP sends a COMMIT message to all neighbors, who then update the local knowledge about their neighborhood and possibly change the radio channel they operate on or instruct individual STAs to reassociate with a different AP.

There are three cases in which the initiating AP will send a WITHDRAW message to its neighbors in order to cancel a reconfiguration attempt. The first case is that the initiator calculates a negative or zero net effect of the reconfiguration proposal. Secondly, it may happen that one of the receivers of an OFFER message is already processing a reconfiguration proposal by a different AP which has not been committed or rejected yet. It then refuses the new OFFER by answering with a BUSY message. Finally, if at least one of the neighbors does not respond to the OFFER within a certain time interval, the initiator will assume the message was lost or the receiver has deactivated.

4.3 Reconfiguration Algorithms

In order to find a reconfiguration that will yield a lower amount of contention, an AP applies an optimization algorithm to the set of APs and STAs within its horizon, including itself. We have experimented both with a problem-specific genetic algorithm (please again refer to [6]) and a greedy heuristic which we termed "balance or conquer". An AP using this heuristic will choose one of the four following actions, depending on which action will have the most positive effect on contention within its horizon:

1. Try to transfer STAs to (from) other APs such that the number of STAs per channel (not per AP!) is roughly the same within the horizon (= balance). Change your own channel, if necessary.
2. Find another AP whose stations you can cover completely and take them all (= conquer), effectively switching the other AP off.
3. Try transferring all stations to other APs, balancing the number of STAs per channel, effectively switching yourself off.
4. If currently switched off, try to take over STAs (starting with the nearest one) from other APs, as long as this does not increase contention. Change your channel, if necessary.

In our experiments the APs used their collected information to instantiate the model in Section 3 and compute the best action.

4.4 Coordination of Reconfigurations

The last building block of our algorithm is concerned with the question *when* APs attempt to find and propose an improved configuration. We have used

both an uncoordinated approach, in which each AP performs reconfiguration attempts as a Poisson process. Furthermore, we have used two token-passing algorithms, where an AP currently holding a token waits for a random time interval before attempting to propose a reconfiguration and passing the token on to a randomly chosen neighboring AP. The two token-based approaches differ in that the first approach starts with a single token that circulates the network, while in the second all APs initially hold a token. When an AP receives a new token from a neighbor while already holding one, the new token is destroyed, so that eventually only one token remains in the network. Lost or destroyed tokens could be replaced by letting each AP generate a new token at a very small rate, which could vary with the amount of contention—and therefore the necessity for a new token—within an AP's horizon.

The rationale behind experimenting with different reconfiguration coordination approaches is that one can expect the global level of contention in the system to decrease more rapidly when a high number of access points concurrently try to find and propose reconfigurations, as is the case with the uncoordinated approach. On the other hand, when reconfigurations are made at different locations of the network at the same time, there is a chance that the effect of one reconfiguration will be counterproductive with respect to another reconfiguration in the long run.

5 Experiments and Results

All experiments were conducted in scenarios with 50 APs and 100 STAs within a 1km by 1km simulation area. In a first step, 16 of the APs were placed to regularly cover the simulation area. Afterwards, the remaining APs were placed uniformly over the simulation area. The location of each STA was chosen by picking an AP randomly and then placing the STA within a distance of 10% to 90% of the radio range of the AP, drawn from a uniform distribution.

We then calculated the path losses between each pair of nodes based on the empirical indoor propagation loss model recommended in ITU-R P.1238-2 [13]. The maximum transmission power s_i for each node was set to 20dBm (or 100mW), which is the maximum power allowed for IEEE 802.11b wireless LANs in Europe. We have set l_i, the minimum signal strength to detect a busy medium, and r_i, the minimum signal strength requirement of a node to -84dBm and -82dBm, respectively, as these are typical values for an Orinoco Gold IEEE 802.11b adapter.

At the start of a simulation run, all APs choose an unused channel or pick one randomly if all are already occupied. All STAs associate with the AP offering the strongest radio signal, as typical for wireless LANs.

Simulations run for a duration of 1 hour of simulation time, each and every simulation run is repeated 10 times with different scenarios.

If no tokens are passed in the network, the generation of reconfiguration attempts per AP is a Poisson process with rate 1. If one or more tokens are present, the holding time of a token is exponentially distributed with mean 1s.

The objective of our first experiment has been to find out how well our distributed algorithm manages to reduce the contention in the network under study. We have therefore run our algorithm on 10 different wireless network scenarios with both the genetic algorithm (GA) as heuristic for finding local reconfiguration potential as well as the balance-or-conquer (B|C) heuristic. In order to study the effect of concurrent reconfigurations versus sequential reconfigurations, we also combined each of our three different reconfiguration coordination approaches with both algorithms: Uncoordinated reconfiguration (0 tokens), token-passing with 1 token, and N initial tokens for each of N access points. Additionally, we have applied a run over 100,000 iterations of our genetic algorithm to serve as an estimate for the best-case behavior and we use standard WLAN as a reference. The resulting average contention values (both absolute and relative decrease compared to WLAN) and their standard deviation are shown in Table 1.

Table 1. Comparison of contention levels achieved by the distributed algorithm using GA and B|C

	WLAN	GA	Local GA			Local B|C		
initial tokens			0	1	N	0	1	N
mean	512.5 (0.0%)	374.5 (-26.4%)	409.8 (-19.8%)	411.5 (-19.3%)	413.5 (-18.9%)	454.0 (-11.1%)	416.8 (-18.2%)	425.3 (-16.6%)
std. error	18.8	7.2	13.6	11.9	10.9	15.9	10.6	11.6

Figure 1 additionally shows the development of the amount of contention over time for one of the simulated scenarios. As the global GA does not necessarily find the global minimum and the true minimum cannot be determined, we have additionally included a (loose) theoretical lower bound (TLB), which we derived in [14].

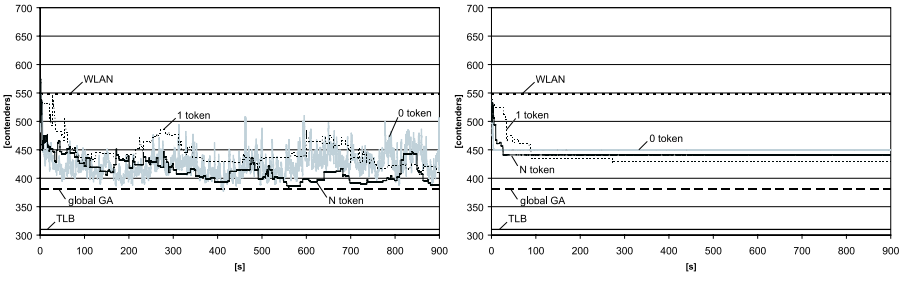


Fig. 1. Performance of GA (left) and B|C (right) as local reconfiguration algorithms compared to global minimum and WLAN

In our simulations, the GA version of our distributed algorithm managed to realize on the average 65.5% of the improvement potential compared to WLAN,

the B|C version 61.8%, both for the 1 token case. This corresponds to a decrease in network-wide contention by 19.3% and 18.2%, respectively. Both versions switched off a significant number of APs to achieve this result (12.2% and 13.6%, respectively). Interestingly, this fact seems to contradict previous findings (e.g. [15]) that load balancing between APs leads to optimal allocations. Note, however, that this is only true if there is no interference between BSSes, i.e. when they are separated spatially or by operating on different channels[14], which is uncommon in highly dense scenarios such as wireless community networks.

Although both versions achieve comparable results, this does not mean that both versions are equally suitable for real-world application. The computational effort per search for a better local reconfiguration is on the order of two magnitudes higher for the genetic algorithm than for B|C, while only achieving slightly better results. Furthermore, the stability of the contention levels is not the same between the two versions as can be directly seen from Fig.1 as well.

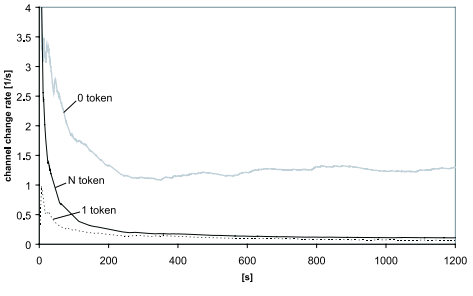


Fig. 2. Channel change rate of GA as local reconfiguration algorithm

We have also observed that the choice of the reconfiguration coordination mechanism has a strong effect on the speed of the improvements in contention, but also on the quality of the attained contention level. Using no coordination between reconfiguration attempts of different APs leads to very quick improvements compared to the 1 token approach. Interestingly, though, in almost all cases the B|C heuristic was able to converge to lower contention levels the slower the rate of reconfigurations was. The N token case was usually somewhere in between, reacting as the uncoordinated case when a large number of tokens was still present, and with time converging to the behavior of the 1 token case as more and more tokens are destroyed. Figure 2 shows the channel changes per second (as a total over the whole network) for the local GA algorithm and the 0, 1, and N token cases, which again supports the aforementioned observations.

Finally, we wanted to find out how important the local negotiation part is for our distributed algorithm. We therefore performed a set of experiments in which we removed the negotiation process, so that an AP finding a better configuration immediately commits the necessary changes instead of sending offers to all other APs within its horizon asking for feedback. The results are shown

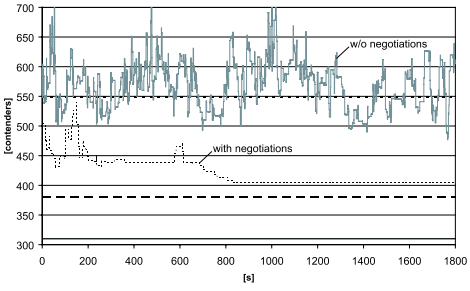


Fig. 3. Comparison of algorithm performance with and without negotiations

in Fig.3 for a single scenario. Indeed, when an AP does not ask its neighbors for possible negative effects of a configuration change, it frequently happens that an AP reconfigures to gain a small improvement, but that this reconfiguration has strong negative effects on the network just outside its horizon. As a consequence, the contention levels heavily fluctuate and may on the average even be higher than with plain WLAN.

6 Conclusions and Outlook

The problem of contention between wireless LANs consisting of a large number of different administrative domains—a common situation in wireless community networks—necessitates some form of self-coordination. In this paper we have taken a first step at tackling the problem of minimizing contention in decentralized wireless community networks, an issue which until now has not received much attention in the literature, but poses a real practical problem to the deployment of emerging large-scale WLANs.

We have proposed a distributed algorithm and protocol for self-coordination of wireless access points from different administrative domains based solely on knowledge about the immediate neighborhood. Experimental results have shown that our distributed algorithm is capable of exploiting 61.8% of the potential for reducing network contention over WLAN, compared to what could be achieved with perfect knowledge. We have also shown that in dense deployments with only few available channels it may be necessary to switch off some APs to reduce contention, rather than performing load-balancing between them. Furthermore, we have found that performing local reconfigurations without feedback from neighboring access points may lead to heavily fluctuating levels of contention which may even be higher than in plain WLAN.

For future work, we perceive the development of even more effective reconfiguration and/or coordination schemes as a short-term goal. We would also like to relax the implicit assumption of cooperative access points towards non-cooperative environments. Currently, we are implementing the presented framework on a set of 4G Access Cubes manufactured by 4G Systems Ltd. in order to be able to investigate its feasibility and scalability in a real-world environment.

References

1. NYCwireless (2006) `http://www.nycwireless.net`.
2. Akella, A., Judd, G., Seshan, S., Steenkiste, P.: Self-Management in Chaotic Wireless Deployments. In: 11th International Conference on Mobile Computing and Networking (MOBICOM '05), Cologne, Germany (2005)
3. WS5100 Wireless Switch Reviewer's Guide. Product brochure, Symbol Technologies (2005) `ftp://symstore.longisland.com/Symstore/pdf/wireless/WS5100ReviewersGuide.pdf` (last access: 2006-01-01).
4. AutoCell—The Self-Organizing WLAN. White paper, Propagate Networks (2003) `http://www.propagatenet.com/resources/docs/whitepaper_autocell.pdf` (last access: 2006-01-01).
5. Matsunaga, Y., Katz, R.: Inter-Domain Radio Resource Management for Wireless LANs. In: IEEE Wireless Communications and Networking Conference (WCNC 2004), Atlanta, Georgia, USA (2004) 2183–2188
6. Zdarsky, F.A., Martinovic, I., Schmitt, J.B.: On Lower Bounds for MAC Layer Contention in CSMA/CA-Based Wireless Networks. In: 3rd ACM/SIGMOBILE International Workshop on Foundations of Mobile Computing (DIALM-POMC'05), Cologne, Germany (2005) 8–16
7. Amaldi, E., Capone, A., Cesana, M., Malucelli, F.: Optimizing WLAN Radio Coverage. In: IEEE International Conference on Communications (ICC 2004), Paris, France (2004) 180–184
8. Leung, K., Kim, B.J.: Frequency Assignment for IEEE 802.11 Wireless Networks. In: 58th IEEE Vehicular Technology Conference (VTC 2003 Fall), IEEE (2003) 1422–1426
9. Ling, X., Yeung, K.: Joint Access Point Placement and Channel Assignment for 802.11 Wireless LANs. In: IEEE Wireless Communications and Networking Conference (WCNC 2005). (2005)
10. Lee, Y., Kim, K., Choi, Y.: Optimization of AP Placement and Channel Assignment in Wireless LANs. In: IEEE Conference on Local Computer Networks (LCN 2002). (2002)
11. Hills, A., Friday, B.: Radio Resource Management in Wireless LANs. IEEE Communications Magazine **42**(10) (2004) 9–14
12. Wang, Y., Cuthbert, L., Bigham, J.: Intelligent Radio Resource Management for IEEE 802.11 WLAN. In: IEEE Wireless Communications and Networking Conference (WCNC 2004), Atlanta, Gergia USA (2004) 1365–1370
13. ITU-R P.1238-2: Propagation data and prediction methods for the planning of radio communication systems and radio local area networks in the frequency range of 900 MHz to 100 GHz (2001)
14. Zdarsky, F.A., Martinovic, I., Schmitt, J.B.: Self-Coordination Mechanisms for Wireless Community Networks. Technical Report 339/05, University of Kaiserslautern, Germany (2005)
15. Kumar, A., Kumar, V.: Optimal Association of Stations and APs in an IEEE 802.11 WLAN. In: Proceedings of the National Conference on Communications (NCC), Kharagpur, India (2005) 1–5

Distributed Opportunistic Scheduling in IEEE 802.11 WLANs

Seong-il Hahm[1], Jongwon Lee[2], and Chong-kwon Kim[1]

[1] School of Electrical Engineering and Computer Science
Seoul National University, Seoul, 151-742, Republic of Korea
{siham, ckim}@popeye.snu.ac.kr
[2] School of Computer Science & Electrical Engineering
Handong Global University, Pohang, 791-708, Republic of Korea
ljw@handong.edu

Abstract. Opportunistic scheduling monitors the receivers' channel states and schedules packets to the receivers in relatively good channel conditions. Opportunistic scheduling can be easily implemented in cellular networks such as the 1xEVDO system because the channel state report function is embedded in the system. To apply opportunistic scheduling to WLANs, deficient of channel report functions, we first devise efficient channel probing mechanisms. Several opportunistic scheduling methods for WLANs have been proposed recently. These previous methods limit the candidate receivers and may not fully realize the potential multiuser diversity gains. In this paper, we develop new opportunistic scheduling called WDOS (Wireless LAN Distributed Opportunistic Scheduling). That is based on a modified RTS/CTS exchange scheme. In WDOS, a sender broadcasts a BRTS (Broadcast RTS) to all receivers. A receiver responds with a CTS after a backoff delay. The value of the backoff delay is determined such that the receivers in relatively better channel conditions acquire channel accesses. We evaluate the performance of WDOS both via an analytic method and via computer simulations. Our performance study shows that WDOS achieves the performance near optimal.

Keywords: WLANs, Opportunistic scheduling, Multiuser diversity, Distributed scheduling, Channel probing, Temporal fairness.

1 Introduction

Dynamic fluctuations of channel quality in wireless networks provide the opportunities to improve the performance of the systems. Channel fluctuations occur both in a short-term scale (small-scale fading) and in a long-term scale (large-scale propagation) [11]. In this paper, we focus on small-scale fading such as Rayleigh and Ricean fading because they are commonly used to describe the flat fading channel characteristics in the outdoor and indoor environment, respectively. Suppose that a sender has packets to send to several receivers. If the sender knows the receivers' channel conditions, it transmits packets to the

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 263–274, 2006.

receiver in the best channel condition at a high data rate. Because receivers in good channel conditions get service, the overall performance of the system improves. The performance gains obtained by exploiting the dynamic fluctuation of channel quality are called multiuser diversity gains [7] or scheduling gains.

Opportunistic scheduling algorithms, which exploit the multiuser diversity, need to know all receivers' channel states. In cellular networks such as 1xEVDO [10], mobile stations (i.e. handset) report their channel qualities to a Base Station (BS) periodically. Based on the reported channel conditions, the BS schedules a packet to the most suitable receiver.

To apply opportunistic scheduling to WLANs, deficient of channel report functions, we first devise efficient channel probing mechanisms. Recently, Medium Access Diversity (MAD) [6] and Opportunistic packet Scheduling and Media Access control (OSMA) [12] have been proposed to exploit multiuser diversity in WLANs. To explicitly probe receivers' channel qualities, both MAD and OSMA use the modified RTS/CTS exchange mechanism. To confine the overhead of channel probing, both methods limit the channel probing to three or four candidates. MAD and OSMA may not be able to fully realize potential multiuser diversity gains because they exclude some receivers in scheduling.

In this paper, we propose a new WLAN opportunistic scheduling algorithm called WLAN Distributed Opportunistic Scheduling (WDOS). Like MAD and OSMA, WDOS also uses a modified RTS and CTS exchange to probe channel conditions. However, WDOS invites all receivers to report their channel conditions without excessive probing overheads and has a potential to fully realize multiuser diversity gains.

A brief description of WDOS is as follows. A sender broadcasts a channel probing message called BRTS (Broadcast RTS) to all receivers. Receiving the probing message, each receiver waits a random backoff period before responding with a CTS frame. The station that has the shortest backoff period will transmit a CTS message first. Hearing the first CTS message, other receivers give up their CTS transmissions. The sender transmits a packet to the station that transmits the CTS message. The backoff period of each receiver is determined by its relative instantaneous channel quality. A station in a better relative channel condition has a shorter backoff delay and has a better chance to be scheduled. By using relative channel quality, not absolute one, WDOS can guarantee temporal fairness even though the average channel qualities of receivers are different.

We have evaluated the performance of WDOS using both an analytical method and computer simulations. The performance results indicate that the throughput of WDOS is 30% higher than that of MAD and OSMA if there are more than ten receivers. The advantage of WDOS becomes more significant as the number of receivers increases. Given that the channel qualities of all receivers are i.i.d. with the same average, the throughput of WDOS approaches to that of the max C/I scheduler [8] and achieves the throughput near maximal. In the case that the average channel qualities of receivers are different, WDOS provides temporal fairness like proportional fair scheduling [5].

The rest of the paper is organized as follows. Section 2 describes several previous results related to our work. Section 3 illustrates the basic framework of WDOS and explains a possible implementation scheme. In Section 4, we provide an analytic model for the performance analysis of WDOS. Section 5 evaluates the performance of WDOS and compares its performance with other opportunistic scheduling mechanisms using both the analytic model and computer simulations. The conclusions are given in Section 6.

2 Related Works

Cellular network systems such as 1xEVDO have an intrinsic channel information report mechanism. But the IEEE 802.11 WLANs do not support the mechanism. Therefore, it is more difficult to adopt opportunistic scheduling in WLANs than cellular network systems.

In spite of the difficulty, two opportunistic scheduling algorithms for WLANs have been proposed recently: MAD [6] and OSMA [12]. Both schemes modify the RTS/CTS exchange to probe channel conditions of selected candidate receivers. In MAD, a sender selects a few candidate receivers and probes the channel states of the candidates by sending a modified RTS frame. MAD explicitly specifies the selected candidates by recording their addresses in the RTS frame. To confine the overhead of channel probing, MAD limits the number of candidates to three. Each candidate receiver responds with a CTS frame specifying its instantaneous channel quality. To avoid CTS response collisions, the receivers transmit CTS frames according to the order that the sender specifies in the RTS frame. Based on the reported channel information, the sender selects a receiver.

OSMA is another opportunistic scheduling method designed for WLANs. Like MAD, a sender selects candidate receivers and transmits a channel probing message to the candidates. OSMA limits the number of candidate receivers to four. When a candidate receiver hears the probing message from a sender, it measures its channel quality and tests if the channel quality is better than a certain threshold. The receiver responds to the probe message only if its channel quality is better than the threshold. As soon as the first response is detected, the probing process terminates and the sender transmits data frames to the receiver that sends the response. OSMA uses a CTS collision avoidance mechanism similar to MAD's.

3 Proposed Scheme

3.1 Framework

Our work begins from the question, "How can we fully realize multiuser diversity gains without excessive overheads of channel probing?" MAD and OSMA fail to fully realize multiuser diversity gains because they limit the number of candidate receivers. Because the probing overheads of MAD and OSMA increase in

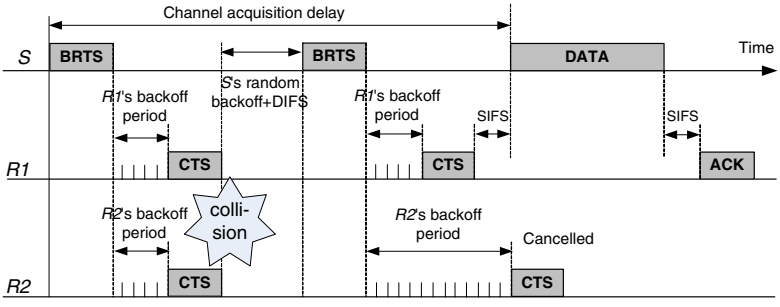


Fig. 1. Channel probing procedure of WDOS

proportion to the number of candidates, these methods cannot expand the number of candidates. Both methods should optimize a trade-off relation between the multiuser diversity gain and the probing overhead. It has been shown that the numbers three and four optimize the trade-off relation in MAD and OSMA, respectively [6],[12].

The essence of opportunistic scheduling for WLANs is the channel probing mechanism. In order to fully achieve multiuser diversity gains, we have to probe all receivers without excessive probing overheads. To break the trade-off relation, we propose a contention-based probing scheme. The scheme, named WDOS, employs the RTS/CTS handshake mechanism with some modifications. A sender broadcasts a Broadcast RTS (BRTS) control frame to all the *active* receivers[1]. Each receiver waits for a time called the backoff period before responding with a CTS control frame. There are the chances that two receivers randomly select the same backoff period and CTS frames collide. Collide or not, the first CTS finishes the current channel probing period. Fig. 1 briefly shows the channel probing procedure of WDOS with a simple example. The sender, S, probes the channel conditions of two active receivers, $R1$ and $R2$, by broadcasting a BRTS frame. $R1$ and $R2$ determine their backoff periods based on estimated channel quality. At first, they have the same backoff time and their CTS frames are collided. After waiting for a binary exponential backoff period, the sender retransmits a BRTS frame. At this time, $R1$ has a shorter backoff period than $R2$, and $R1$ gains the channel. We define the channel acquisition delay as the time from the first BRTS transmission to the beginning of DATA transmission. If a CTS collision occurs, the acquisition delay becomes longer.

3.2 Backoff Period

The performance of WDOS depends on the effectiveness and efficiency of the mechanism that selects the CTS backoff periods. A good backoff mechanism must satisfy two requirements; maximum multiuser diversity gains and minimum overheads of channel probing. In addition, we pursue the third requirement, fairness of scheduling. The first and third requirements are easy to accomplish; the

[1] A station is called an active receiver to which a sender has pending data frames.

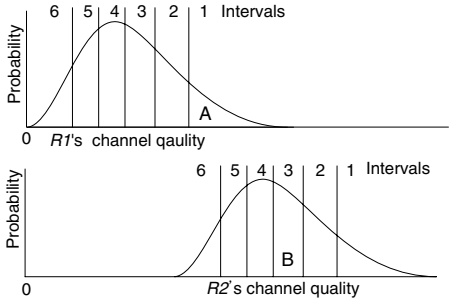


Fig. 2. Channel quality distribution and backoff mechanism

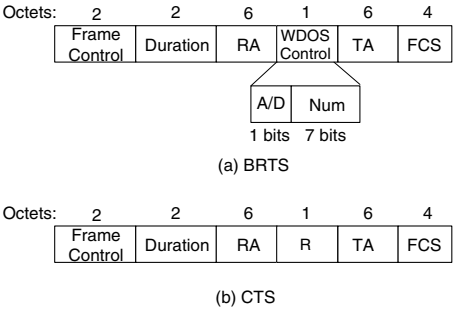


Fig. 3. WDOS control frame formats

first by assigning shorter backoff delays to receivers in better channel qualities, and the third by using *relative*, not absolute, channel qualities.

Let us elaborate the backoff mechanism with an example. For the sake of simplicity, we suppose that two receivers' channel quality follows the identical distribution with different averages. Each p.d.f. is divided into a fixed number of intervals of equal probability as shown in Fig. 2. If a receiver is in interval 1, it can respond to the BRTS frame without backoff. In interval 2, it should wait one slot, and so on. Suppose $R1$ and $R2$ are in the first interval (denoted by 'A') and in the third interval (denoted by 'B'), respectively. Even though absolute channel quality of $R2$ is better than that of $R1$, $R1$ grasps the channel because its relative channel quality is better than $R2$'s.

The number of partitions, L, is an important parameter that ultimates the efficiency of the channel probing mechanism. Large values of L reduce the chance of collisions but delay the first CTS response. Small values of L exert the exactly opposite effects on the collision probability and the responsiveness. Apparently, the optimal values of L increase in proportion to the number of receivers, N. The question is "Is the relation linear?". Our performance study indicates that the relationship is practically linear. Section 5 reveals the relationship in a greater detail. Another concern is the continual collisions; two or more receivers in the same relative channel position collide in each of consecutive channel probing periods if their relative channel positions persist. There are several methods that solve the problem. One is to add a random factor to the backoff delay and another is the binary exponential backoff mechanism. For simplicity, WDOS adopts the former method. Let M be the randomization parameter. The backoff delay of a receiver in the i^{th} interval is determined as $\big((i-1) * M + rand[0, \cdots, M-1]\big) * SlotTime$,where $SlotTime$ is one backoff slot time.

WDOS supplies a fail-safe mechanism against abnormal operations. One abnormal condition is the failure of BRTS frame transmission due to collisions or sudden channel degradations. To prevent the sender from waiting for CTS for a prolonged time, WDOS specifies a parameter B_{max} which is the maximum number of slots before the sender stops the current probing period and

starts a new one. We can set B_{max} to a value much smaller than the theoretical limit, $L * M - 1$, because the probability that all N receivers are in the poorest channel condition is very small. Moreover, we can bypass the data transmission opportunities in poor channel condition by adopting small B_{max}.

Another factor that we should consider is the hidden terminal problem. The delayed CTS mechanisms [6][12] may suffer from an additional hidden terminal problem. A CTS frame delayed more than $EIFS - 2 * SIFS - T_{CTS}$ could induce collisions, where T_{CTS} is the CTS transmission time. The hidden terminal problem does not occur in the infrastructure mode operation, the main application target of WDOS. Even in the ad-hoc mode, the hidden terminal problem is scarcely observed in our performance study. Due to the limited space, the results are omitted.

3.3 Structure of Control Frames and Active Receiver Management

WDOS uses variants of the RTS/CTS handshake for channel probing. The frame formats of BRTS and modified CTS frames are shown in Fig. 3. The BRTS control frame contains two additional fields, A/D (Add/Drop) and Num. The A/D flag combined with the RA field manages a set of active receivers. When a sender has data frames to send to a currently dormant receiver, it activates the receiver by recording the receiver's address in the RA field and setting the A/D flag to 'Add'. Deactivation is more complex than activation and we develop two methods: an explicit and an implicit method. The explicit method records the address of deactivated node in the RA field and sets the A/D flag to 'Drop'. The explicit method is usually used to subdue receivers that wrongly think they are active. The implicit method uses the "More Data" flag specified in the IEEE 802.11 standard [3] to continue or stop the states of existing active stations. To deactivate, the sender notifies a receiver to switch to an inactive state by clearing the "More Date" flag. As a measure of fail-safe, the sender reconfirms the activeness of receivers by recording each of their addresses in a round robin manner. The Num field denotes the number of active receivers. The CTS control frame again is augmented with two fields, R and TA; R (Rate) specifies the desirable data rate and TA (Transmitter Address) is the address of the station transmitting the CTS frame.

4 Analysis

This section describes an analysis that derives the throughput of WDOS. To make the analysis simple, we make several assumptions. First, we assume that there are a fixed number of active receivers and there always are packets to send to each receiver. We assume each station can hear each other and there is no hidden terminal problem; anlaysis studies focus on the infrastructure mode. As shown in Section 3, WDOS repeats cycles which consist of up to four phases: the random backoff phase before BRTS, the BRTS transmission phase, the CTS resolution phase, and the frame transmission phase. Only the third phase, the CTS resolution phase, is different from the basic IEEE 802.11 standard from in terms of analysis.

4.1 Average CTS Resolution Time

When an active station receives a BRTS frame, it determines the backoff period based on its relative channel quality. In case of a CTS collision, the channel probing mechanism repeats until a success. Recall that a channel quality p.d.f. is partitioned into L intervals with the equal probability of $1/L$, and each interval consists of M slots. The probability that k receivers transmit CTS frames in the i^{th} interval, $P_{CTS}(i,k)$, is

$$P_{CTS}(i,k) = {}_N\mathrm{C}_k\Big(\frac{1}{L}\Big)^k\Big(1-\frac{i}{L}\Big)^{N-k} \qquad i \in (i,L),\ k \in (1,N). \tag{1}$$

Because the first CTS finishes the channel probing period, there should be no CTS transmissions before the i^{th} interval. Once a station selects an interval, it randomly chooses one integer from an interval $[0,...,M-1]$. A collision occurs if two or more stations select the same interval and the same random number. Let k be the number of stations that select the same interval. The conditional probability that a collision-free transmission of a CTS frame occurs at the j^{th} slot, $P_S(j|k)$, is

$$P_S(j|k) = {}_k\mathrm{C}_1\frac{1}{M}\Big(1-\frac{j}{M}\Big)^{k-1} \qquad k \in (1,N),\ j \in (1,M). \tag{2}$$

The conditional probability of collision at the j^{th} slot, $P_C(j|k)$, is

$$P_C(j|k) = \Big(1-\frac{j-1}{M}\Big)^k - P_S(j|k) - \Big(1-\frac{j}{M}\Big)^k \qquad k \in (1,N),\ j \in (1,M). \tag{3}$$

The probability that the first CTS is successfully transmitted in the j^{th} slot of the i^{th} interval, $P_{S-CTS}(i,j)$, is given as

$$P_{S-CTS}(i,j) = \sum_{k=1}^{N} P_{CTS}(i,k)P_S(j|k) \qquad i \in (1,L),\ j \in (1,M). \tag{4}$$

Similarly, the probability that CTS frames collide in the j^{th} slot of the i^{th} interval, $P_{C-CTS}(i,j)$, is

$$P_{C-CTS}(i,j) = \sum_{k=1}^{N} P_{CTS}(i,k)P_C(j|k) \qquad i \in (1,L),\ j \in (1,M). \tag{5}$$

The average successful CTS resolution time, $\mathrm{E}[T_{S-CTS}]$, is given as

$$\mathrm{E}[T_{S-CTS}] = \sum_{i=1}^{L}\sum_{j=0}^{M-1} P_{S-CTS}(i,j) * \Big(\big((i-1)*M+j-1\big)*\sigma + T_{CTS}\Big), \tag{6}$$

where T_{CTS} is the CTS transmission time and /sigma is the slot time. On the other hand, the average time of CTS collisions, $\mathrm{E}[T_{C-CTS}]$, is

$$\mathrm{E}[T_{C-CTS}] = \sum_{i=1}^{L}\sum_{j=0}^{M-1} P_{C-CTS}(i,j) * \Big(\big((i-1)*M+j-1\big)*\sigma + T_{CTS}\Big). \tag{7}$$

Note that due to the variable data rate, the number of bytes transmitted during the same time duration varies. The probability that a receiver with the channel quality of the i^{th} interval is successfully selected, $P_{S-CTS}(i)$, is determined as

$$P_{S-CTS}(i) = \sum_{j=0}^{M-1} P_{S-CTS}(i,j). \tag{8}$$

The average data size to be transmitted in a single cycle is represented as

$$\mathrm{E}[D] = \sum_{i=1}^{L} D(i) * P_{S-CTS}(i), \tag{9}$$

where $D(i)$ is the average data size transmitted in the i^{th} interval. $D(i)$ varies depending on the channel conditions because a sender transmits data frames to each receiver for a fixed equal time duration in WDOS. $P_S(i)$ and $D(i)$ can not be decoupled because the value of $P_S(i)$ and the transmission rate are correlated. Equation (9), which considers the channel dependent throughput, reflects the multiuser diversity gains.

4.2 Saturation Throughput of the Proposed Scheme

Let P_{tr} be the probability that there is more than one transmission attempt in a slot and P_{S-BRTS} be the probability of a successful BRTS frame transmission. T_{C-BRTS} denotes the time wasted for an unsuccessful BRTS transmission. Let $\mathrm{E}[T_S]$ and $\mathrm{E}[T_C]$ be the average time consumed for a successful and unsuccessful CTS transmission, respectively. Applying the same method used for the analysis of the basic IEEE 802.11 MAC [1], we express the saturated throughput of WDOS, S, as

$$S = \frac{P_{S-BRTS}\mathrm{E}[D]}{(1-P_{tr})\sigma/P_{tr} + (1-P_{S-BRTS})T_{C-BRTS} + P_{S-BRTS}(\mathrm{E}[T_S] + \mathrm{E}[T_C])}. \tag{10}$$

Note that $P_{S-BRTS}\mathrm{E}[D]$ is the average size of successfully transmitted data frames in one cycle. The denominator of Equation (10) is the average cycle time. The first term is the average backoff time of the IEEE 802.11 DCF. The second term represents the average time wasted for each BRTS collision. $T_{C-BRTS} = T_{BRTS} + DIFS$, where T_{BRTS} is the transmission time for a BRTS frame.

The last term is the average time duration for the CTS resolution and data transmission in the case of a successful BRTS transmission. Even after a BRTS frame is transmitted successfully, WDOS suffers from CTS collisions. The last term, which consists of two parts $\mathrm{E}[T_S]$ and $\mathrm{E}[T_C]$, reflects this fact. $\mathrm{E}[T_S]$, the sum of the expected time of a successful CTS resolution and the expected time of a following data transmission, is expressed as $\mathrm{E}[T_S] = \mathrm{E}[T_{S-CTS}] + \sum_i P_{S-CTS}(i)T_S(i)$, where $T_S(i) = T_{BRTS} + SIFS + T_D(i) + DIFS$ and $T_D(i)$ is the average time duration required to transmit frames in the i^{th} interval. $\mathrm{E}[T_C]$, the expected time of an unsuccessful CTS resolution, is given as $\mathrm{E}[T_C] =$

$\mathrm{E}[T_{C-CTS}] + \sum_i \sum_j P_{C-CTS}(i,j) T_C$, where $T_C = T_{BRTS} + SIFS + DIFS$. For example, if n frames can be transmitted in the i^{th} interval, then $T_D(i)$ is given as $T_D(i) = n * (SIFS + H + T_{payload}(i) + SIFS + T_{ACK})$, where H and $T_{payload}(i)$ are the transmission time for the frame header and payload, respectively. T_{ACK} is the ACK transmission time.

5 Performance Evaluations

We conducted analyses and ns-2 based [9] simulations to evaluate the performance of WDOS. The target system is the IEEE 802.11a which supports eight data rates from 6Mbps to 54Mbps [4]. We limit the value of B_{max} to $\min(L * M - 1, 45) * SlotTime$. The size of all data frames is fixed to 1500 bytes. Each simulation result is obtained from 20 repetitions, but the confidence intervals are omitted because they all are too small.

5.1 Effect of L and Multiuser Diversity

We investigated the effects of the number of intervals, L, an important parameter that balances the trade-off relation between collisions and responsiveness, using the analytic model. We assume that all channels follow the Rayleigh fading model with the same average. To pin point the effect of L, eliminating the random effect, we assume $M = 1$.

Two interesting aspects regarding the parameter L are the effect of N on the optimal values of L and its sensitivity. Fig. 4 shows the optimal values of L at different values of N. Because the optimal L increases almost linearly as N increases, we denote the optimal values of L as cN, where c is the slope of the graphs in Fig. 4. From this figure, c is three or four. Now, let us examine the sensitivity of L. Fig. 5 shows the throughput as a function of L for the case of $N = 25$ when the average channel SNR is -72dBm. The throughput increases sharply as L increases from 25 to 54. Beyond $L = 54$, the throughput increases rather slowly and the peak performance is obtained at $L = 107$. The throughput decreases slowly as the number of intervals increases beyond $L = 107$. From this graph, we can deduce that the throughput is not sensitive to L when L ranges from 54 to 150. That is, if we let $L = cN$ and c ranges from 2 to 6, the performance of WDOS is not sensitive to the parameter c.

Fixing $c = 4$ and $M = 1$, we compared the analysis and simulation results to validate the analysis. Fig. 6 shows the throughput as a function of the number of active receivers when all the receivers have the same average channel quality of -72dBm or -75dBm. Analysis and simulation results match well in all cases confirming the accuracy of the analysis. The multiuser diversity gains increase as the number of receivers increases. Note that the 3dB difference of channel quality does not make the 3dB throughput difference because of Medium Access Control (MAC) and physical layer overheads.

5.2 Performance Comparison

We compared the performance of WDOS to those of MAD and OSMA via computer simulations. For proper comparisons, we tuned up the MAD and OSMA

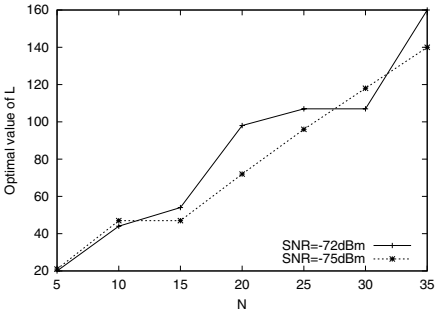


Fig. 4. Optimal values of L at the different average channel qualities

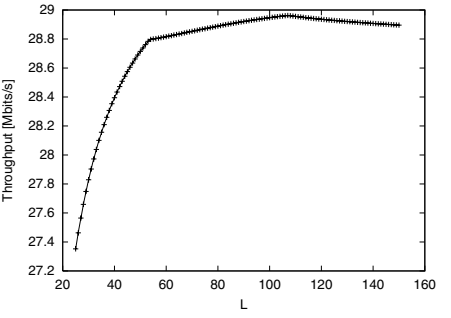


Fig. 5. Throughput with various L when N=25 and SNR_{avg} = -72dBm

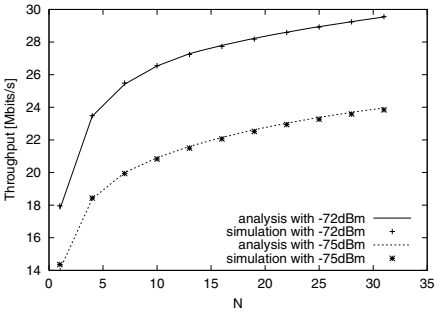


Fig. 6. Throughput: analytic vs. simulation results

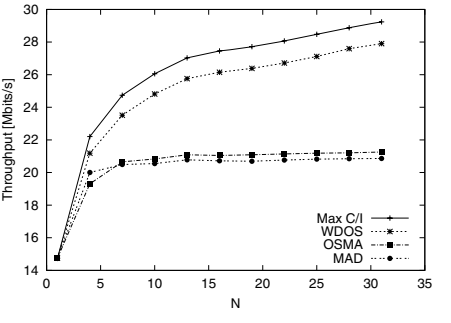


Fig. 7. Throughputs when the number of receivers increases from 1 to 31

protocols. MAD selects candidate receivers in a round-robin manner and chooses the final winner based on the proportional fair (PF) scheduling. In OSMA, the threshold of each receiver is set to a 70 percentage of its average channel quality. We also evaluated the performance of two algorithms, the max C/I scheduler and the PF scheduler. We assume that these two schedulers know the channel conditions of all the receivers with the overhead of one BRTS/CTS exchange. The max C/I scheduler achieves the theoretical maximum throughput [8] while the proportional fair (PF) scheduler provides temporal fairness [2]. We consider the Doppler shift [11] in evaluating the performance. In the case of long coherence time (typical indoor environments), WDOS may experience the performance degradation due to consecutive CTS collisions if $M = 1$. To resolve these consecutive collisions, M must be larger than one. In the following simulations, we fix M=2 and c=3.

Throughput Performance. In this suite of simulations, channels have i.i.d. Rayleigh fading with a 1Hz Doppler shift while the average signal quality at each

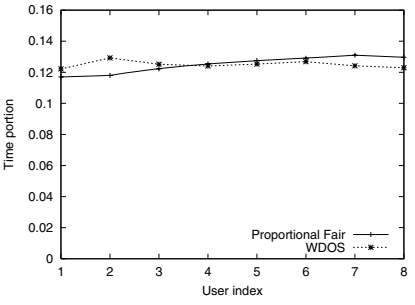


Fig. 8. Temporal fairness

receiver is -72dBm. Fig. 7 shows the throughput of WDOS, MAD, OSMA, and a max C/I scheduler as a function of the number of receivers. The throughput of all the scheduling algorithms increases as N increases from 1 to 5. While the throughput of WDOS and the max C/I scheduler increases further beyond $N = 5$ as N increases, the throughput of MAD and OSMA saturates at around $N = 7$. These results indicate that MAD and OSMA fail to fully realize multiuser diversity gains because they limit the candidate receivers. However, WDOS, which invites all receivers, fully achieves the multiuser diversity gains. When N reaches to 30, the throughput of WDOS is about 34% more than that of MAD and OSMA.

Temporal Fairness. In order to evaluate temporal fairness, we set up a simulation environment, where eight receivers have i.i.d. Rayleigh fading with a 4Hz Doppler shift. Eight receivers have different average channel conditions; -82dBm (user1), -81dBm (user2), $\cdots$, -75dBm (user8). Fig. 8 depicts the time portions consumed by each user under PF scheduling and WDOS. Both scheduling algorithms assign the almost equal time-share (1/8) to each receiver. This reflects that the channel-aware backoff mechanism of WDOS guarantees the same access probability to all receivers even if their average channel conditions are different.

6 Conclusions

In this paper, we proposed a novel opportunistic scheduling algorithm called WLAN Distributed Opportunistic Scheduling (WDOS) for WLANs. In order to probe channel conditions, WDOS uses a modified RTS/CTS handshake, where each active receiver transmits a CTS frame after its own channel-aware backoff expires. Even if this channel-aware backoff mechanism invites all active receivers to report their channel conditions, the channel probing overhead is small since the backoff mechanism adopts a contention-based scheme. In addition, because the first respondent has the relatively best instantaneous channel quality among all the receivers, WDOS fully achieves multiuser diversity gains. Both analysis and simulation results indicate that WDOS outperforms MAD and OSMA.

When the number of active receivers reaches to 30, WDOS achieves up to 34% throughput improvement in the indoor environments. WDOS also has the property of temporal fairness; receivers evenly share the time resource regardless of different average channel conditions.

Acknowledgements

This work was, in part, supported by the Brain Korea 21 Project in 2006. This work was, in part, supported by grant No.R01-200400010-37202005 from the Korea Science & Engineering Foundation. The ICT at Seoul National University provided research facilities for this study.

References

1. G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE JSAC in Commun., vol.18, no.3, pp.535-547, Mar. 2000.
2. J. M. Holtzman, "CDMA forward link waterfilling power control," Proc. IEEE VTC 2000-Spring, Tokyo, Japan, pp.1663-1667, Jan. 2000.
3. IEEE Computer Society LAN/MAN Standards Committee, "Part 11: Wireless LAN Me-dium Access Control (MAC) and Physical Layer (PHY) Specifications," ANSI/IEEE Std 802.11, 1999 Edition.
4. IEEE Computer Society LAN/MAN Standards Committee, "Part 11: Wireless LAN Me-dium Access Control (MAC) and Physical Layer (PHY) specifications. High-speed Physi-cal Layer in the 5 GHz Band," IEEE Std 802.11a-1999(R2003). (Supplement to IEEE Std 802.11-1999).
5. A. Jalali, R. Padovani, and R. Pankaj, "Data Throughput of CDMA-HDR a High Effi-ciency-High Data Rate Personal Communication Wireless System," Proc. IEEE VTC 2000-Spring, Tokyo, Japan, pp.1854-1858, Jan. 2000.
6. Z. Ji, Y. Yang, J. Zhou, M. Takai, and R. Bagorodia, "Exploiting Medium Access Diversity in Rate Adaptive Wireless LANs," Proc. ACM MOBICOM 2004, Philadelphia, Pennsyl-vania, pp.345-359, Sep. 2004.
7. R. Knopp and P. Humblet, "Information capacity and power control in single cell multiuser communications," Proc. IEEE ICC 1995, Seattle, WA, pp.331-335, Jun. 1995.
8. A. Kogiantis, N. Joshi, and M. O. Sunay, "Effects of Scheduling on Transmit Diversity Performance in 1xEV-DV," Lucent Contribution to 3GPP2 TSG-C Standards Body, Dec. 2000.
9. NS-2, http://www.isi.edu/nsnam/ns, 2005.
10. Qualcomm, Inc., "1xEV: 1x Evolution IS-856 TIA/EIA Standard Airlink Overview," Nov. 7, 2001, Revision 7.2.
11. T. S. Rappaport, "Wireless Communications: principles and practice," 2nd Edition, Pren-tice Hall.
12. J. Wang, H. Zhai, and Y. Fang, "Opportunistic Packet Scheduling and Media Access Control for Wireless LANs and Multi-hop Ad Hoc Networks," Proc. IEEE WCNC 2004, Atlanta, Georgia, Mar. 2004.

Mean Effective Gain of Compact WLAN Genetic Printed Dipole Antennas in Indoor-Outdoor Scenarios

Pedro Luis Carro and Jesus de Mingo

University of Zaragoza,Electronic Engineering and Communications Department, Zaragoza 50018, Spain
plcarro@unizar.es, mingo@unizar.es
http://diec.unizar.es

Abstract. Two dual-printed dipole antennas for WLAN applications operating in the 802.11 a/b/g (2.4-2.5 Ghz and 4.9-5.875 GHz) frequency bands are presented. Genetic Algorithm optimization (GA) is applied first, to a classical dual band printed dipole antenna schema. Later on, a pre-fractal technique is proposed on the larger strip and electromagnetic parameters are re-optimized to achieve a more compact radiator. Frequency performance of both antennas is introduced showing a VSWR$<$ 1.5 for a input impedance of 50 Ohms. Finally, the mean effective gain (MEG) is worked out considering several scenarios. Results for both antennas for typical indoor and outdoor environments are given using the statistical angle of arrival behavior of such environments.

Index terms - WLAN, printed dipole antennas, genetic algorithms, Mean Effective Gain.

1 Introduction

In the last few years, the development of wireless local area networks (WLANs) was one of the main research focus in the information and communications field. Therefore, a strong effort in antenna design to provide wireless coverage with low cost has been a key factor to accomplish the WLAN development.

In this paper, a radiating element is designed to adopt the standard printed circuit board (PCB) substrate and production technology. The uniqueness of the design comes from an evolving optimization procedure applied to a classical dual printed dipole antenna (DPDA) [1] used previously in 2 and 3G base station systems combined with a pre-fractal topology [2] to reduce the size. Additionally, since the antenna is oriented to be used in a mobile device, a traditional approach to evaluate the electromagnetic performances is not enough to predict the overall behavior in a wireless scenario. The Mean Effective Gain (MEG) [3], is a recently defined parameter to include the mobile channel characteristics (those referred to spatial and polarization properties). This parameter is computed for the radiating elements placed in typical scenarios: indoor and indoor-outdoor urban.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 275–283, 2006.

In section II, the antenna geometries and design outlines are presented, showing the evolution of the GA applied. In section III, classical electromagnetic parameters (S-parameters, Gain) coming from the optimization are showed. In section IV , MEG results are presented. Finally, a conclusion is provided.

2 Dual Printed Dipole Antenna (DPDA) Designs with GA

2.1 Antenna Geometries of PDA

Fig.1 shows a schematic drawing of the antennas showing the genes involved in the genetic optimization. In the classical DPDA, two printed strip dipoles of different lengths, with the arms printed on opposite sides of an electrically thin dielectric substrate are connected through a parallel stripline (PS). In the case of the pre-fractal printed dipole antenna (PF-DPDA), the first iteration of a fractal tree is applied to the longer element so that the size can be reduced. In order to achieve an optimal dual-frequency radiator, the line polarity between the radiating elements must be inverted. The antennas were designed on a dielectric substrate of height $h = 1.6$mm, relative permittivity $\epsilon = 4.5$ and loss tangent $\tan(\delta) = 0.02$.

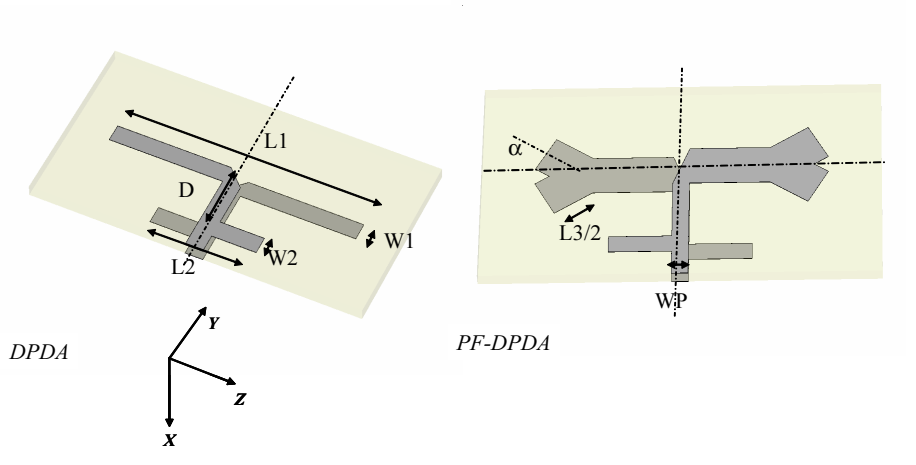


Fig. 1. Return Losses of DPDA and PF-DPDA

2.2 Evolutive Optimization (GA) Results

A genetic optimization method was applied for each geometry (DPDA PF-DPDA). Six and eight genes are codified using 30 bits in a binary codification, respectively. A simple GA with typical parameters $p_{cross} = 0.65, p_{mut} = 0.01$, size population of 30 individuals was let to evolve during 150 generations in DPDA and 100 generations in PF-DPDA. The *Fitness function* was:

$$F = |R_{in}(\omega_1) - 50| + |R_{in}(\omega_2) - 50| + |R_{in}(\omega_1) - R_{in}(\omega_2)| + |X_{in}(\omega_1)| + |X_{in}(\omega_2)| \quad (1)$$

Table 1. Optimum chromosomes found by GA simple

Gene	DPDA(mm)	PF-DPDA(mm)
L1	45.054	26.2694
L2	19.3643	21.3248
D	12.5259	13.2189
W1	5.5733	5.9203
W2	2.7896	2.5660
WP	2.9568	2.5019
L3	–	14.8525
α	–	30.9282

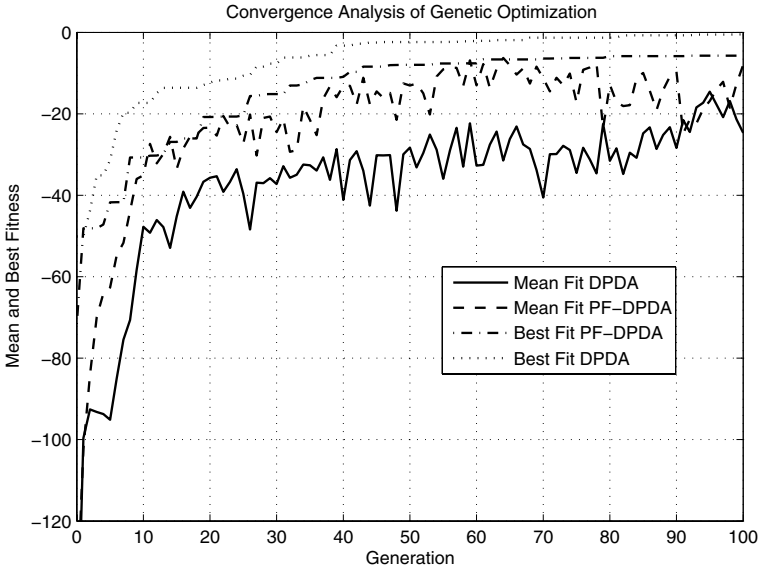


Fig. 2. Gain Pattern of PF-PDA Antenna

where $Z_{in}(\omega_i) = R_{in}(\omega_i) + jX_{in}(\omega_i)$ is the antenna input impedance at ω_i frequency.

With this fitness function, a resonant 50Ω input impedance at both frequencies is looked for. The frequencies chosen for WLAN where 2.45 and 5.4 GHz. The antenna parameters were obtained from a standard MoM simulation program. Table 1 shows the optimized parameters for each antenna and Fig. 2 the fitness function convergence towards the optimum.

As observed, computing the Size Reduction as

$$\text{size reduction} = \frac{L_1^{DPDA} - L_1^{PFDPDA} - L_3/2\cos(\alpha)}{L_1^{DPDA}} \tag{2}$$

a 27.55% of compactness is achieved thanks to the pre-fractal method.

3 Classical Performances for the Radiating Configurations

The classical analysis of antennas comprises, among others, these main quantities: the S-parameters, impedance bandwidth and the gain radiation pattern.

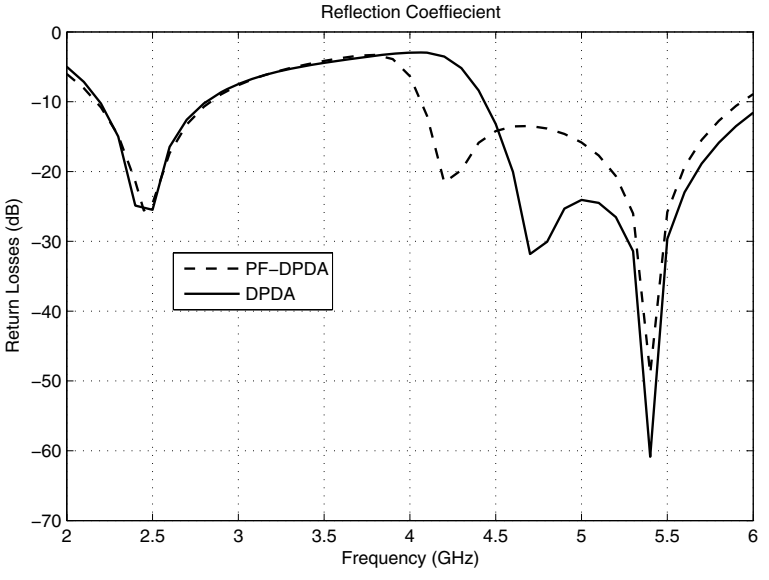


Fig. 3. Return Losses of DPDA and PF-DPDA

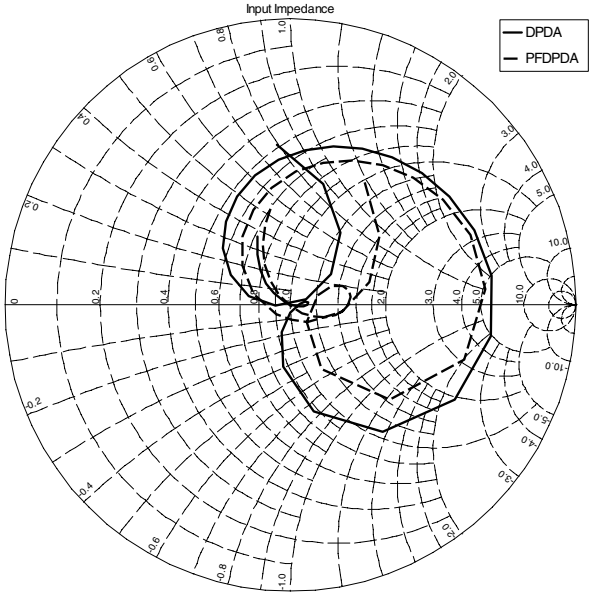


Fig. 4. Return Losses of DPDA and PF-DPDA

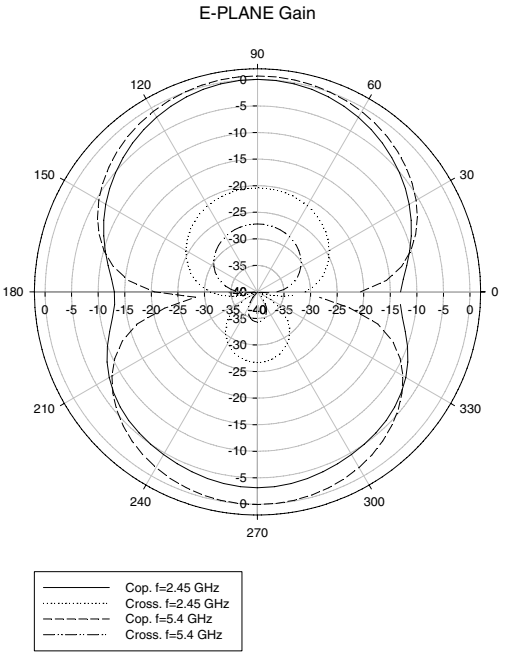


Fig. 5. Gain Pattern of PF-DPDA Antenna

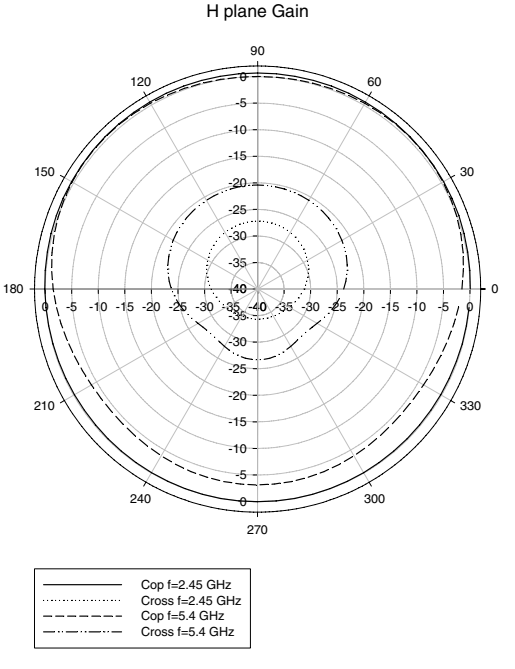


Fig. 6. Gain Pattern of PF-DPDA Antenna

The S_{11} is plotted in Fig.3-4. Considering a $|\Gamma| < -15dB$ as bandwidth criteria, it is obvious that the antennas are radiating in the whole WLAN frequencies specified.

Regarding the pattern, Fig.5-6 represents the E and H plane cuts.It is observed that the antennas have almost an omnidirectional diagram in the lower band while in the upper band the pattern is more directive. Table 2 summarizes the classical performances.

Table 2. Antenna main traditional parameters

Parameter	DPDA	PF-DPDA
Bandwidth WLAN 1 (MHz)	220	360
Bandwidth WLAN 2 (MHz)	900	1455
Directivity WLAN 1 (dBi)	1.73	1.71
Directivity WLAN 2 (dBi)	4.6	3.38
Gain WLAN 1 (dBi)	0.54	0.67
Gain WLAN 2 (dBi)	1.11	0.52

4 Effective Gain Analysis in WLAN Environments

4.1 Method of Analysis

As mentioned, the MEG is a statistical measurement of the antenna performance in a multipath enviroment. The mean power received from the antenna can be obtained from the radiation patterns and the statistics of the channel using this concept. The MEG of an antenna, which is defined as the ratio of the mean received to the mean incident power at the antenna, can be calculated from [4],

$$MEG = \oint \left[\frac{\Gamma}{1+\Gamma} P_\theta(\Omega) G_\theta(\Omega) + \frac{1}{1+\Gamma} P_\phi(\Omega) G_\phi(\Omega) \right] d\Omega \tag{3}$$

where G_θ and G_ϕ are the θ and ϕ polarized components of the antenna power gain pattern, Ω is the solid angle (θ, ϕ), P_θ and P_ϕ are the θ and ϕ components of the angular density functions of the incoming plane waves.Γ is the crosspolarization power ratio, defined as the ratio of the mean received power in the vertical polarization to the mean received power in the horizontal polarization. The crosspolarization power ratio (Γ or also known as XPD) varies considerably, depending on the surrounding enviroment. Thus, these values must be concreted according to the mobile application of interest.

4.2 Incident Wave Statistics for WLAN Environments

As a result of the large amount of interest in the wireless channel, several probability density functions have been proposed [5], [6], [7], validated through measurements. First results were related to the temporal properties of the propagation environment, and finally, a focus in the angular power distribution motivated

by the emerging MIMO systems has brought several models for the incident wave statistics. In the case of the XPR, it is shown that its value is between 0 dB and 9 dB in most cases, although in some enviroments can achieve 11 dB.

When a WLAN indoor enviroment it is considered, two possible scenarios may be of interest:

Indoor Environment
The antenna is assumed to be working inside a building. Measurements [8] have shown that the power azimuth spectrum P_ϕ is best modeled by a Laplacian function for both polarization. A Gaussian function for the elevation is assumed. Therefore, for the DPDA and PF-DPDA antennas:

$$P_\phi(\theta,\phi) = A_\phi e^{-\left|\frac{\sqrt{2}\phi}{\sigma}\right|} e^{-(\theta-[\pi/2-m_H])^2/2\sigma_H^2}, 0 \le \theta \le \pi, 0 \le \phi \le 2\pi \quad (4)$$

$$P_\theta(\theta,\phi) = A_\theta e^{-\left|\frac{\sqrt{2}\phi}{\sigma}\right|} e^{-(\theta-[\pi/2-m_V])^2/2\sigma_V^2}, 0 \le \theta \le \pi, 0 \le \phi \le 2\pi \quad (5)$$

For these pdfs, suitable statistic moments will be $\sigma = 24°, \sigma_H = 9°, \sigma_V = 11°$ and $m_V = 4°, m_V = 2°$. MEG will be study for XPRs between 0 and 11, although measurements point out values around 7 dB.

Indoor-Outdoor Environment
The antenna is assumed to be working outside a building, but close to the point access system. This corresponds to traditional gaussian pdfs in elevation and uniform distribution in azimuth. Therefore, for the DPDA and PF-DPDA antennas:

$$P_\phi(\theta,\phi) = A_\phi e^{-(\theta-[\pi/2-m_H])^2/2\sigma_H^2}, 0 \le \theta \le \pi, 0 \le \phi \le 2\pi \quad (6)$$

$$P_\theta(\theta,\phi) = A_\theta e^{-(\theta-[\pi/2-m_V])^2/2\sigma_V^2}, 0 \le \theta \le \pi, 0 \le \phi \le 2\pi \quad (7)$$

In both cases, A_θ and A_ϕ are constants that must fulfill:

$$\int_0^{2\pi}\int_0^{\pi} P_\theta(\theta,\phi)\sin\theta d\theta d\phi = \int_0^{2\pi}\int_0^{\pi} P_\phi(\theta,\phi)\sin\theta d\theta d\phi = 1 \quad (8)$$

For these pdfs, suitable statistic moments will be $\sigma_H = 8°, \sigma_V = 15°$ and $m_V = 1°, m_V = 2°$. MEG will be study for XPRs between 0 and 11, although measurements point out values around 11 dB.

4.3 Results

Fig. 7 shows results for MEG in indoor-outdoor environment, for both frequency bands. As expected, if XPR increases, the MEG is improving approaching to theoretical Gain.

As seen, the antenna performance is worse at the higher frequency than at lower,and the antennas have almost the same MEG,with slightly differences. Fig 8 presents the results for the PF-DPDA in both enviroments. It is revealed that, in the case of the indoor environment, the MEG is slightly worse. As the Laplacian distribution is sharper than the uniform in the center, the indoor MEG is lower compared to the outdoor MEG.

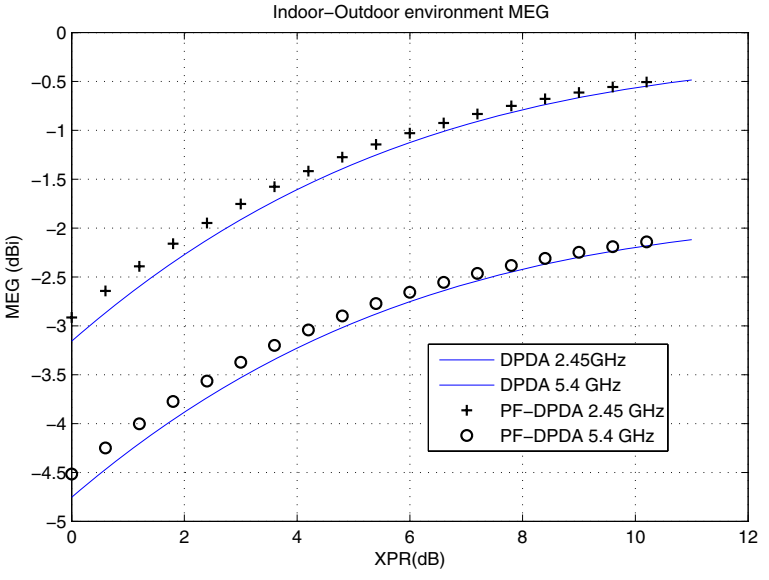


Fig. 7. MEG in indoor-outdoor environment

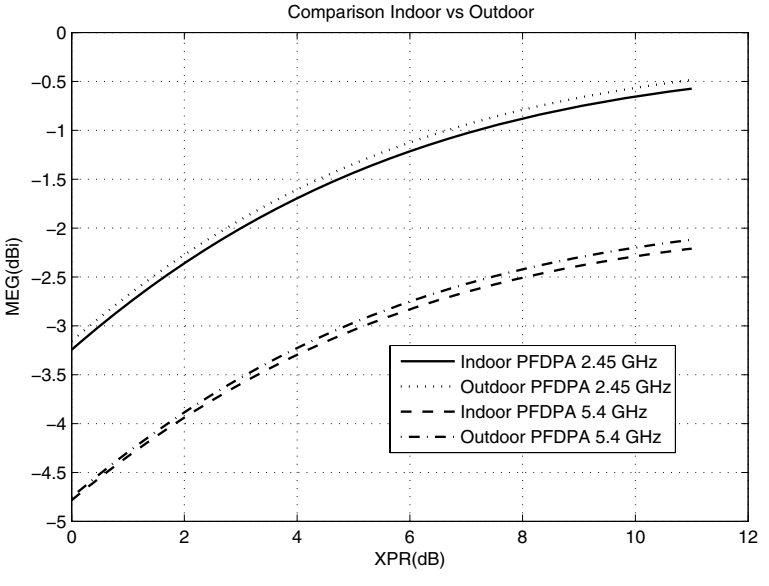


Fig. 8. MEG in indoor-outdoor environment

5 Conclusion

This paper shows a novel genetically pre-fractal printed dipole antenna for WLAN frequency bands. The antenna is analyzed in classical terms showing good performances in both bands. Additionally, the Mean Effective Gain is

obtained two typical scenarios, revealing an identical performance in the compacted antenna and the standard.

Acknowledgement

This work has been funded by the Ministry of Education and Science and the European funds of regional development (FEDER) under the project TEC 2004-04529/TCM and the European Union through the Program Marco under the project PULSERS PHASE-2 (Pervasive Ultra-wideband Low Spectral Energy Radio Systems PHASE 2).

References

[1] F. Tefiku and C. A. Grimes, Design of Broad-Band and Dual Band Antennas Comprised of Series-Fed Printed-Strip Dipole Pairs, IEEE Trans. Antennas and Propagat. Vol.48,No 6, June, 2000.

[2] J.S. Petko and D. H. Werner, Miniature reconfigurable three-dimensional fractal tree antennas, IEEE Trans. Antennas and Propagat. Vol.52,No 8, Aug, 2004.

[3] de Mingo, J.; Valdovinos, A.; Gutierrez, F.; Gonzalez, J.M., Inverted-F antenna with parasitic elements for TETRA handset, Vehicular Technology Conference, 1999. VTC 1999 - Fall. IEEE VTS 50th Volume 3, 19-22 Sept. 1999

[4] Douglas,M.G.; Okoniewski, M.; Stuchly, M.A, A planar diversity antenna for handheld PCS devices,Vehicular Technology, IEEE Transactions on Volume 47, Issue 3, Aug. 1998

[5] Kalliola, K.; Sulonen, K.; Laitinen, H.; Kivekas, O.; Krogerus, J.; Vainikainen, P., Angular power distribution and mean effective gain of mobile antenna in different propagation environments,Vehicular Technology, IEEE Transactions on Volume 51, Issue 5, Sept. 2002

[6] Waldschmidt, C.; Wiesbeck, W., Compact wide-band multimode antennas for MIMO and diversity,Antennas and Propagation, IEEE Transactions on Volume 52, Issue 8, Aug. 2004

[7] Hajian, M.; Nikookar, H.; der Zwan, Fv.; Ligthart, L.P., Branch correlation measurements and analysis in an indoor Rayleigh fading channel for polarization diversity using a dual polarized patch antenna,Microwave and Wireless Components Letters, IEEE Volume 15, Issue 9, Sept. 2005

[8] pencer, Q.H.; Jeffs, B.D.; Jensen, M.A.; Swindlehurst, A.L., Modeling the statistical time and angle of arrival characteristics of an indoor multipath channel,Selected Areas in Communications, IEEE Journal on Volume 18, Issue 3, March 2000

Experimental Assessment of a Cross-Layer Solution for TCP/IP Traffic Optimization on Heterogeneous Personal Networking Environments

Luis Sánchez*, Jorge Lanza, and Luis Muñoz

University of Cantabria, E.T.S. Ingenieros Industriales y de Telecomunicación, Avda. de Los Castros s/n, 39004, Santander, Spain
{lsanchez, jlanza, luis}@tlmat.unican.es
Departamento Ingeniería de Comunicaciones, E.T.S. Ingenieros Industriales y de Telecomunicación, Avda. de Los Castros s/n, 39004, Santander, Spain
lsanchez@tlmat.unican.es

Abstract. Future wireless communication scenarios will be characterized by the heterogeneity in terms of coexisting wireless access technologies. Many mobile terminals will support different air interfaces and in order to provide true multi-mode operation, the sole use of IP protocol is not enough. We present in this document the Universal Convergence Layer that residing on top of the different air interfaces offers a single interface to IP while supporting the cross-layer optimization of user data flows as well as many other key functionalities in personal networks communications. This document describes and discusses the implementation of this framework over real platforms. Furthermore, the results of the measurement campaign carried out to assess the benefits introduced by the dynamic interface selection mechanism implemented at the UCL will be also presented. The results obtained will allow us to extract conclusions about the appropriateness of the solution adopted.

Keywords: Cross-layer optimization, Measurement campaign, Validation results, Convergence layer.

1 Introduction

Next generation wireless systems should provide to the user access to a broad range of services in a transparent way, making the technology embedded in the natural surroundings. Accomplishing this goal requires efficient cooperation between heterogeneous networking technologies and different frameworks. A large number of wireless access technologies are envisaged to coexist in future wireless communication spaces. So, the necessary methods for them to interwork seamlessly have to be deployed. In this sense, the corresponding MAC and link layer protocol(s) should be accessed from upper layer protocols and applications independently of the type of technology that is being used (in the same way upper layer protocols and applications access the underlying protocol stack through the socket interface for data purposes).

* Corresponding author.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 284 – 296, 2006.

The concept of isolating the upper-layers from underlying wireless technologies and thus providing real multi-mode can be achieved by introducing a Universal Convergence Layer (UCL) [1]. The UCL can be seen in a twofold approach. It mainly will act as an enabler for backward and forward compatibility by defining a common interface towards the network layer while managing several different wireless access technologies independently of their PHY and MAC layers. On the other hand, the UCL can also enable the cross-layer optimization paradigm. Its privileged location within the protocol stack gives the UCL the possibility to support the information to flow both bottom-up (e.g. use of SNR information for enriching the decision process in an ad hoc routing algorithm) and top-down (e.g. tune of MAC parameters depending on the battery status or QoS requirements).

Although the flexibility of the solution proposed in [1] regarding the UCL is broad and presents a framework which represents a foothold for many schemes aiming at optimizing the overall system performance, this paper is focused on the implementation work carried out and the characterization and validation of a dynamic interface selection mechanism that exploits the cross-layer optimization paradigm to enhance the performance of TCP/IP data flows over heterogeneous wireless environments.

The paper briefly introduces in Section 2 the high-level protocol stack specifying the main requirements and challenges the UCL must tackle. It also sketches the UCL's implementation framework over Linux-based laptops. In Section 3, the validation analyses made to the UCL are presented. The scenario where the measurement campaign was carried out will be presented. In this section, both the location and the communication equipment will be described providing a rationale to its selection and the fundaments by which the results obtained can be extrapolated to other situations. The performance that would be obtained without the UCL will be firstly analyzed and then compared with the behavior exhibited when the UCL is loaded. Finally, Section 5 presents some conclusions derived from the evaluation carried out.

2 Protocol Architecture and Implementation Aspects

The capability of working in a heterogeneous environment is a must for future personal networks. This heterogeneity will be mainly reflected in terms of the different air interfaces that will coexist and need to cooperate to provide the users with services located at their neighborhood and beyond. Additionally, multimode devices (i.e. supporting several wireless interfaces) will be common in these scenarios requiring additional schemes to handle this heterogeneity.

Moreover, secure communications has to be granted. Authenticity and privacy are the main issues that are to be assured for personal communications.

The purpose of the UCL is to house not only the mechanisms in order to interact with the underlying technologies in a transparent way, but also those schemes based on the cross-layer optimization paradigm which could benefit themselves by the direct communication with the lower and upper layers.

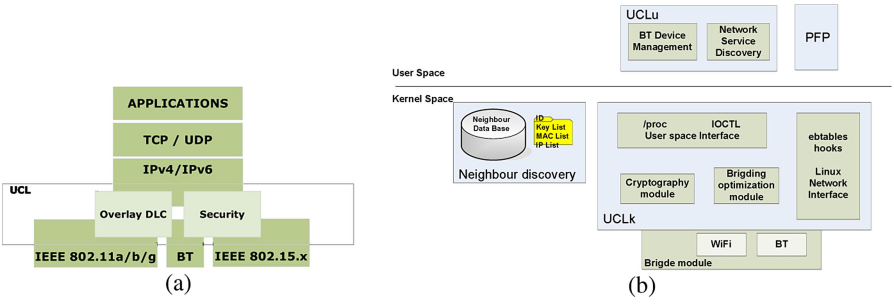


Fig. 1. UCL High-Level architecture *(a)*; UCL low level architecture specification *(b)*

The architecture shown in Fig. 1 aims at fulfilling the requirements aforementioned while enabling the settlement of some machinery that exploits the cross-layer paradigm in order to optimize the overall system behavior. Note that its design is foreseen as being highly scalable and thus it is based on a common skeleton to which different modules could be added in order to provide with specific functionalities. The two main building blocks that currently form the UCL architecture are:

- Overlay DLC & Path Optimization

UCL's privilege location in the network stack offers the possibility of defining a common interface towards the network layer, hiding the complexity of the different wireless access technologies, and providing the mechanisms to handle data transmission over different interfaces, taking responsibility away from the network layer.

Additionally, the different wireless access technologies will present a different behavior depending on the channel conditions. While IEEE 802.15.3 [2] or IEEE 802.11n [3] offer very high throughputs over short ranges, other technologies are able to reach higher coverage reducing their maximum binary rate. Taking this into account, it has been implemented within the UCL a mechanism to dynamically select the most appropriate air interface to use for communicating with another device whenever multiple choices are possible. The selection has been based on the status of the channel and the maximum available bandwidth following a cross-layer optimization approach.

- Security

The security systems of the various radio technologies differ not only in terms of the encryption algorithms used, but also on the security information they require from the upper layers. The UCL will be a common framework where the deployment of different security strategies could be housed. In this sense, the security requirements imposed will be realized and enforced using the available radio interfaces.

The following sections will depict more in depth the Linux features that has been used in the UCL implementation.

2.1 Linux Ethernet Virtual Device

The idea of a virtual interface can be useful to implement special-purpose processing on data packets while avoiding hacking the network subsystem of the kernel. In this

sense, the virtual interface could be considered as a tool for customizing network behavior. To control the operation mode of the virtual device (add new ports, enable security issues, …) user space programs interact with kernel modules.

From the aforementioned, one or multiple interfaces can appear as one large interface to the participating hosts by binding them to the same virtual network interface. In our case the virtual network interface will manage all the PAN wireless network interfaces. In this sense the UCL resembles a network bridge which could be considered the baseline for UCL development. However, to achieve the purposes foreseen within MAGNET in terms of heterogeneity, security and data transfer management it is necessary to extend these functionalities and adapt its behavior to the new requirements.

2.2 Security Libraries

In the last Linux kernel versions some cryptographic features that allow applying encryption and decryption to packets without having to queue them to user space have been included.

The UCL will cope with security at a link level, before the packet is actually sent to its destination. To handle packets at this level it is necessary to develop some kernel code and cryptographic algorithms have to be used. Cryptographic operations will be used for deriving a session key based on a mutual authentication mechanism. Taking into account these premises, Linux kernel cryptographic modules offer the suitable algorithms (DES, AES, HMAC, SHA, MD5, …).

3 Validation Results

This section presents the results obtained from the measurement campaign carried out in order to prove and validate the benefits introduced by the UCL solution. A full set of tests were carried out in order to show the UCL aptitudes and communication optimization. The selection of optimal interface mechanism based on the channel conditions experienced by the different wireless interfaces managed by the UCL has been deeply analyzed.

During this measurement campaign we have focused on the analysis of TCP/IP traffic performance over a typical personal networking heterogeneous environment.

3.1 Measurement Campaign Scenario

This section describes the environment in which the measurement campaign was carried out. Fig. 2 shows the scenario where all the tests were performed. Four different locations were selected, each of them showing gradually worse channel behavior.

The measurement environment is a typical offices location but can also resemble an in home scenario. Basically, the charter of selecting this environment was to test the UCL on a real world scenario which would allow us to draw conclusions that can be directly mapped on real situations a user may experience.

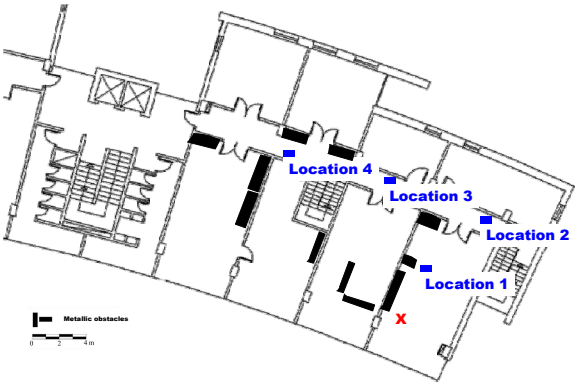


Fig. 2. Measurement campaign environment

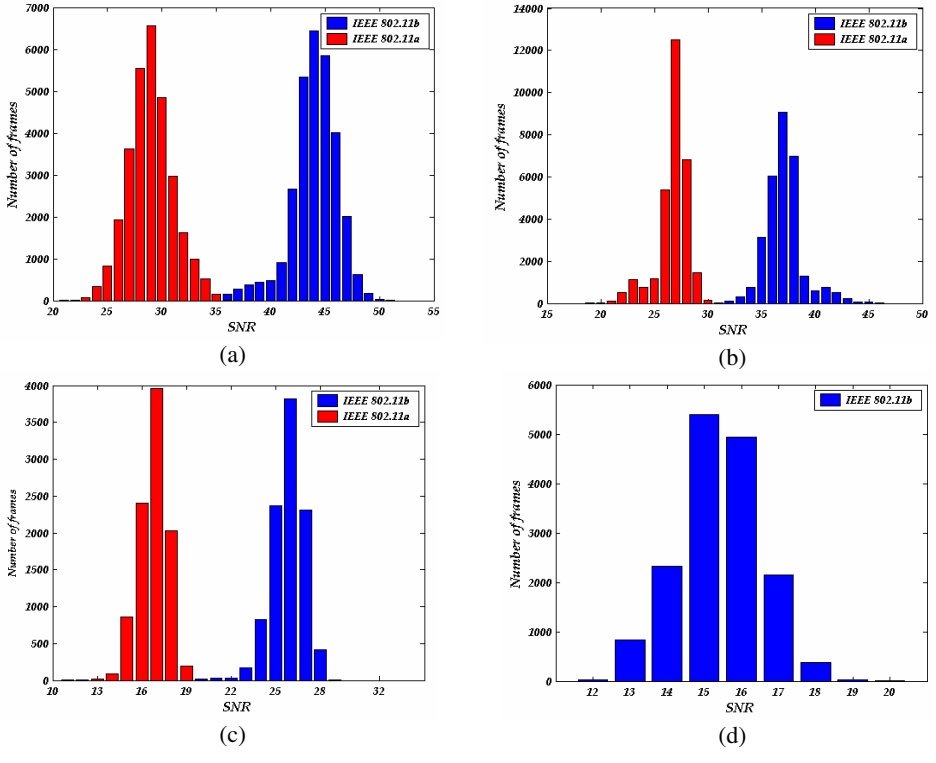


Fig. 3. Location 1, 2, 3 and 4 (*(a), (b), (c)* and *(d)* respectively) received frames SNR distribution

Our setup consisted of two laptops – both running Linux. One of them was always placed on the red mark while the other was moved between the different locations shown in Fig. 2. The laptops were equipped with two wireless interfaces, namely

IEEE 802.11a cards based on the Atheros chipset, and built-in IEEE 802.11b/g cards based on the Intel chipset.

The first task carried out during the measurement campaign was to analyze the scenario and present the characteristics of each of the selected locations. During the measurement campaign IEEE 802.11a and IEEE 802.11b were used in order to resemble the heterogeneity in data rates and behavior against channel conditions. Hence, the generic conclusions obtained could be extrapolated to other wireless technologies.

Fig. 3 shows the distribution of the signal to noise ratio on each of the locations. These distributions were obtained by sending a 30 seconds long UDP traffic flow between the two laptops and analyzing the SNR registered on the receiver of this flow. Table 1 summarizes the main parameters of the received SNR (Signal to Noise Ratio) on each of the locations. Note that in the Location 4, there are results available only for IEEE 802.11b since channel conditions for IEEE 802.11a were so bad that the measurements couldn't be used for appropriately describe the location.

As can be seen, the selected locations offers a good range of situations ranging from very good channel conditions to poorer ones that will produce a deep degradation of the communications.

Table 1. Channel characteristics parameters

	IEEE 802.11b		IEEE 802.11a	
	Mean SNR	**Std. deviation**	**Mean SNR**	**Std. deviation**
Loc. 1	**43.94**	**2.29**	**28.97**	**2.06**
Loc. 2	**37.09**	**1.76**	**26.75**	**1.46**
Loc. 3	**25.83**	**1.14**	**16.78**	**0.99**
Loc. 4	**15.4**	**1.13**	**---**	**---**

Link quality metrics such as ETX (Expected Transmission Count Metric) [4], MTM (Medium Time Metric) [5], WCETT (Weighted Cumulative Expected Transmission Time) [6], etc. have been proposed as metrics to estimate the link quality and replace the minimum hop count metric, which is widely used by current routing protocols, to select paths in order to increase network capacity. However, there are still some limitations for applying these metrics to real implementations such as the pure collection of the parameters required to calculate them. Besides, the SNR has been proven to be an adequate representative of the link quality [7][8]. Hence, our approach can be considered valid, not only because it matches the wireless channel behavior quite faithfully but also because the implementation carried out is ready to support richer metrics with which better decisions can be made.

3.2 TCP Traffic Characterization

As already said, the laptops used during the measurement campaign were equipped with two wireless interfaces which behave differently in the various locations studied. The measurements carried out firstly presents the performance obtained when using each of them. This approach will allow us to show the performance shown by each of the wireless interfaces to be used and decide the appropriate threshold level of SNR at

which change the output interface to send the traffic through. At the end of the section some mobility scenarios will be presented where the output interface is changed dynamically depending on the SNR experienced in each moment.

The tests performed in this section shows the performance obtained in each of the different locations when an FTP session is established for transferring a 10 Mbytes file from one laptop to the other.

TCP traffic is highly affected by packet loss. Since TCP was designed for wired networks where packet loss is always assumed as collisions provoked by channel congestions, the congestion avoidance mechanisms of TCP forces the transmitter to stop when these situations are detected. Nevertheless, in wireless channels, normally, packet loss is due to channel impairments for which stopping the transmitter is pointless.

During the TCP traffic characterization several parameters will be studied in order to have the most accurate picture of the communication performance. Basically, these parameters refer to the TCP retransmissions as they are the main responsible of performance degradation.

3.2.1 Location 1

Table 2 presents the results obtained during the tests carried out in Location 1. As can be seen, in both cases the channel can be considered ideal maintaining the number of retransmission up to a reduced level. Besides, the errors occur in an independent fashion preventing the transmitter to misleading situations which might provoke long transmitter idle times. Under these ideal conditions, the best choice would be the IEEE 802.11a interface. Note that the selection of interface in the case of TCP traffic is quite direct since the only parameter to compare is the final throughput. Additionally, we will also look at the variability of the results in order to evaluate the best choice on each location.

Table 2. Location 1 TCP statistics

# Test		Throughput (Mbps)	Out of order pkts	Idle time max (ms)	Max # of retx	# retx
IEEE 802.11a	***(1)***	27,71	61	40	1	61
	(2)	28,36	76	7,5	2	78
	(3)	27,83	80	40	2	82
	(4)	28,38	70	7,7	1	70
	(5)	28,11	83	9,6	2	85
IEEE 802.11b	***(1)***	5,11	11	112,2	1	11
	(2)	5,11	5	108,7	1	5
	(3)	5,08	7	105,3	1	7
	(4)	5,09	7	103,1	1	7
	(5)	5,10	5	105,8	1	5

3.2.2 Location 2

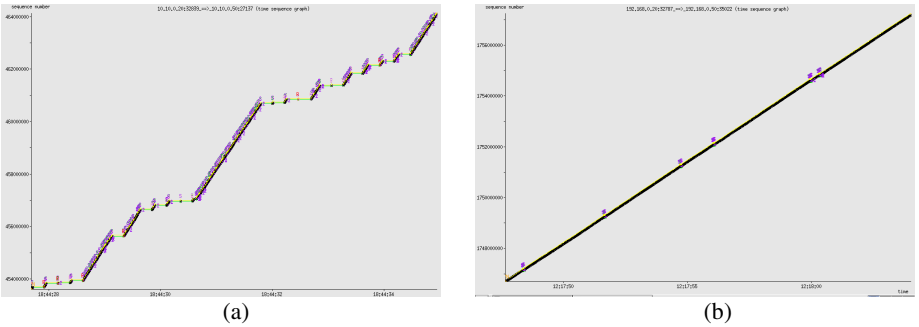
Table 3 presents the results obtained during the tests carried out in Location 2. Although the performance is severely reduced due to the poorer channel conditions, in most of the cases IEEE 802.11a behaves better than its counterpart. As can be seen,

the number of retransmissions is increased considerably, but they still occur in a quite independent manner (*Max # of retx* represents the maximum number of consecutive retransmissions) which doesn't trigger the TCP congestion avoidance mechanisms. Hence, the performance is not completely tear down and remains better than IEEE 802.11b, which on contrary remains stable in an almost error-free channel.

Table 3. Location 2 TCP statistics

# Test		Throughput (Mbps)	Out of order pkts	Idle time max (ms)	Max # of retx	# retx
IEEE 802.11a	***(1)***	9,01	238	411,9	3	272
	(2)	11,56	285	231,7	2	301
	(3)	9,72	406	409,9	2	425
	(4)	13,70	159	401,9	3	173
	(5)	3,43	311	6431	7	356
IEEE 802.11b	***(1)***	5,13	8	108,9	1	8
	(2)	5,12	7	109,7	1	7
	(3)	5,11	2	108,8	1	2
	(4)	5,11	6	104,2	1	6
	(5)	4,94	8	118,1	1	8

Fig. 4 shows two time-sequence graphs presenting IEEE 802.11a and IEEE 802.11b behavior in Location 2 respectively. As can be seen, IEEE 802.11b presents a linear performance where the slope corresponds to 5 Mbps, typical in ideal channel conditions. On contrary, IEEE 802.11a presents a disrupted behavior mixing periods where the communication is almost perfect with others where the transmitter is idle. Nevertheless, the channel is not such bad and IEEE 802.11a beats its counterpart.



(a) (b)

Fig. 4. Location 2 TCP traffic time-sequence graphs *(a) for IEEE 802.11a* and *(b) for IEEE 802.11b*

However, test #5 using 802.11a interface draws the attention to the vulnerability of TCP protocol to channel impairments [9]. In this test, a burst of lost packets (look at *Max # of retx*) results on a large idle time (almost 6.5 seconds) which makes the throughput to decrease even below 802.11b level. In this sense, it would be interesting to distinguish different thresholds for different types of traffic (e.g. TCP and UDP).

The UCL enables this possibility, allowing also the definition of more complex QoS functions which would allow to the decision to be taken to not only take into account the transport layer protocol but also application specific requirements and not only SNR but also other link layer parameters.

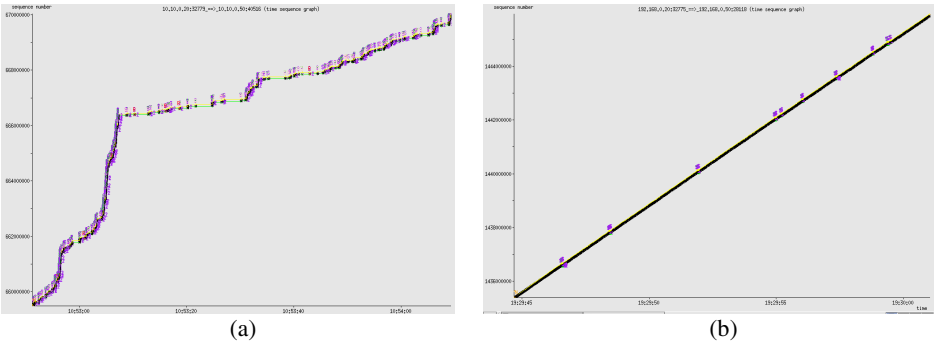
3.2.3 Location 3

Table 4 presents the results obtained during the tests carried out in Location 3. The very poor channel conditions observed when using 802.11a results on high packet loss and a large number of retransmissions, which triggered the congestion avoidance mechanisms of TCP, leading to long periods where the transmitter remains silent. Besides, it is important to note the high variability that was experienced during the measurement campaign. This variability makes it really difficult to perform full measurements since in several tests the FTP session was aborted due to expiration of maximum idle time.

Table 4. Location 3 TCP statistics

# Test		Throughput (Mbps)	Out of order pkts	Idle time max (ms)	Max # of retx	# retx
IEEE 802.11a	***(1)***	1,08	678	1663,7	5	928
	(2)	3,50	428	815,9	3	545
	(3)	2,20	220	6463	6	267
	(4)	4,00	344	819,9	4	421
	(5)	1,30	313	7657,4	4	402
IEEE 802.11b	***(1)***	5,16	10	102,5	1	10
	(2)	5,06	24	112,7	1	24
	(3)	5,10	24	92,4	1	24
	(4)	5,13	12	88,1	1	12
	(5)	5,14	14	98,8	1	14

A typical example of the behavior of each interface can be seen in Fig. 5. The transmissions over IEEE 802.11a presents a poor performance spotted continuously with transmitter idle periods. The 802.11a graph corresponds with test #2 which does



(a) (b)

Fig. 5. Location 3 TCP traffic time-sequence graphs *(a) for IEEE 802.11a* and *(b) for IEEE 802.11b*

not have a really long maximum idle time (see for example test #5) but the amount of retransmissions needed prevents from achieving higher throughputs. It is clear that under these circumstances the most suitable choice should be the 802.11b interface.

3.2.4 Location 4

Table 5 presents the results obtained during the tests carried out in Location 4. As can be seen, on Location 4 statistics only for 802.11b can be presented. The situation shows such a poor channel conditions that it is impossible to finish any FTP session using the 802.11a interface. Opposite, 802.11b shows an acceptable behavior reducing its throughput but maintaining a good performance. Note that even using 802.11b the radio channel impairments causes a large number of retransmission.

Table 5. Location 4 TCP statistics

# Test		Throughput (Mbps)	Out of order pkts	Idle time max (ms)	Max # of retx	# retx
IEEE 802.11b	***(1)***	1,68	430	3197,9	4	544
	(2)	4,34	136	415,9	2	147
	(3)	1,83	499	835,7	4	606
	(4)	4,09	130	465,9	3	147
	(5)	2,19	392	461,9	3	467

The evolution of the time-sequence graphs in this case is not so linear like in the former locations but it remains free from too long periods of transmitter inactivity.

3.2.5 Dynamic Interface Selection Based on SNR

The selection of the optimal output interface for each individual packet may depend on multiple parameters (e.g. application specific QoS requirements, channel congestion, etc.). Thus the decision process within the UCL can be made as complex as desired.

In our case, we have used a simpler approach to validate the optimization achieved with the UCL by deciding which interface to send the packet through only taking into account the SNR observed in each of the channels. Examining the characterization performed to TCP traffic, the SNR level used as threshold for switching from one output interface to the other was set to 25 dB in the UCL implementation.

Table 6. Moving scenario TCP statistics

UCL (optimal interface selection enabled)		IEEE 802.11a		IEEE 802.11b	
# Test	**Throughput (Mbps)**	**# Test**	**Throughput (Mbps)**	**# Test**	**Throughput (Mbps)**
1	19,7	**1**	12,7	**1**	5,15
2	19,1	**2**	13,5	**2**	5,14
3	19,3	**3**	11,3	**3**	5,17
4	17,3	**4**	11,9	**4**	5,15
5	20,1	**5**	12,0	**5**	5,17

The tests performed for validating the optimal selection of the output interface consisted on moving one of the laptops from Location 1 to Location 4 and back again while the other remained fixed on the red mark in Fig. 2. This test was run using first the UCL with its optimal interface selection option enabled, then the IEE 802.11a interface only and finally the IEEE 802.11b interface only. Each case was repeated five times.

Table 6 presents the results from the different tests carried out. In these tests, a 1500 bytes TCP packets flow lasting 40 seconds was exchanged between the two laptops.

It is important to note, that in all the tests performed we have tried to repeat exactly the same movements maintaining the same speed all along the path. Nevertheless, the results might vary slightly from one to the other due to the impossibility of replicating exactly the movement. However, the different repetitions of the same experiment allow us to extract valid conclusions.

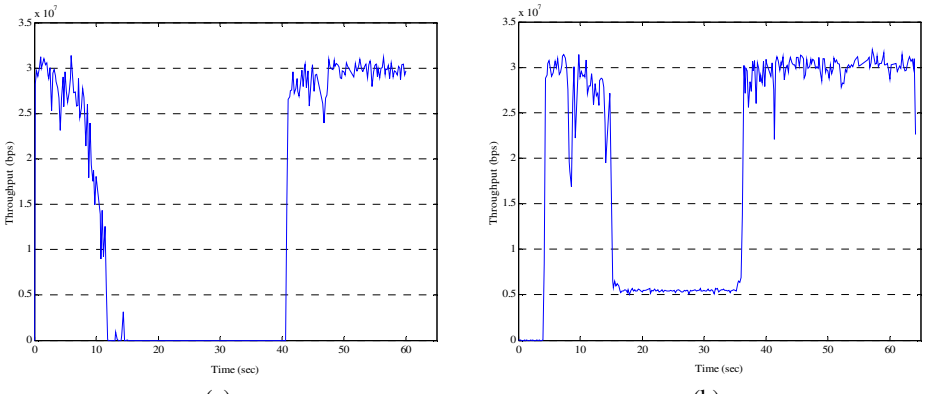


Fig. 6. Moving scenario TCP traffic immediate throughput evolution using the IEEE 802.11a, and UCL (*(a)* and *(b)* respectively)

In the case of TCP, the erroneous interpretation of packet loss as channel congestion triggers the TCP congestion avoidance mechanisms makes the throughput to be reduced significantly when using only the IEEE 802.11a.

As can be seen in Fig. 6 there is a period of time in which the instantaneous throughput is 0 Mbps. This period corresponds to the time in which the laptop is between Locations 3 and 4 plus the amount of time that the transmitter needs to start sending packets again, after its congestion avoidance mechanisms have removed the corresponding timeouts.

Fig. 6 shows how the UCL swaps the interface used from 802.11a to 802.11b before the conditions are so degraded that the congestion avoidance mechanisms are triggered so the throughput is maintained using the IEEE 802.11b and immediately after the laptop ingresses again in the area where the channel conditions are good, it is able to swap again to the higher binary rate interface without having to wait for congestion avoidance timeouts to expire.

When the transmission is forced to go through the 802.11b the throughput is always maintained stable around 5 Mbps.

As can be seen, the UCL always selects the most appropriate interface in each moment exploiting the advantages of the two options. When the channel is good uses the interface which offers higher bandwidth but when it detects that the channel is starting to deteriorate switches to the interface that offers stronger behavior against radio channel impairments.

4 Conclusions

In the above sections we have presented a complete set of results obtained from different measurements campaigns that have proven the feasibility of the implemented UCL and the optimization achieved through its use.

This work has presented a complete experimental assessment of the benefits that a cross-layer optimization approach can bring up in the field of wireless communications. The optimizations introduced by the UCL, through the selection of the most appropriate output interface based on channel status have been presented in the case of using TCP traffic.

Although there has been a lot of interest on this sort of solutions, they lack from an experimental evaluation. In this sense, one of the main contributions of this work is that it presents the results of a purely experimental approach, showing that, in spite of the shortcomings of current available "off-the-shelf" technologies, it is possible to practically consider and integrate cross-layer optimization concepts over these technologies.

It has been proven how the UCL enables the dynamic adaptation to the channel conditions resulting on a substantial performance enhancement.

During the different validation tests, they have been identified possible enhancements that can be supported by the UCL although they have not been already implemented. In this sense, and although the SNR has proven to give interesting results, future work will add new parameters to the decision process, such as network load or trust relationships between different nodes; investigating on optimal link cost functions.

References

[1] IST-507102, My Personal Adaptive Global NET, MAGNET, Deliverable D.3.3.2a, "MAC/RRM Schemes for PANs", July 2004.

[2] IEEE std 802.15.3, Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs).

[3] IEEE std 802.11n. IEEE Standard for Information technology—Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment: Higher throughput improvements.

[4] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing", 9th ACM International Conference on Mobile Computing and Networking, San Diego, California, September 2003

[5] B. Awerbuch, D. Holmer, H. Rubens, “High Throughput Route Selection in Multi-Rate Ad Hoc Wireless Networks”, First Working Conference on Wireless On-demand Network Systems 2004.

[6] R. Draves, J. Padhye, and B. Zill, “Routing in Multi-radio, Multi-hop Wireless Mesh Networks”, ACM International Conference on Mobile Computing and Networking 2004

[7] J.P. Pavon and S. Choi, "Link adaptation strategy for IEEE 802.11 WLAN via received signal strength measurement," IEEE ICC 2003, vol.2, pp.1108–1113, May 2003.

[8] K. Balachandran, S. R. Kadaba, and S. Nanda "Channel Quality Estimation and Rate Adaptation for Cellular Mobile Radio". IEEE Journal on Selected Areas in Communications, Vol. 17, No. 7, pp. 1244-1256, 1999.

[9] L. Muñoz, M. Garcia, J. Choque, R. Aguero and P. Mähönen, “Optimizing internet flows over IEEE 802.11b wireless local area networks: A performance-enhancing proxy based on forward error correction,” IEEE Communication Magazine, pp. 60–67, December, 2001.

Cross-Layer Loss Differentiation Algorithms to Improve TCP Performance in WLANs

Stephane Lohier[1], Yacine Ghamri Doudane[2], and Guy Pujolle[3]

[1] IUT- University of Marne la vallée, 77420 Champs sur Marne – France
lohier@univ-mlv.fr
[2] Computer Engineering Institute - IIE - 18, allée Jean Rostand 91025 Evry Cedex – France
Ghamri@iie.cnam.fr
[3] LIP6 - University of Paris VI - 8, rue du Capitaine Scott 75015 Paris – France
Guy.Pujolle@lip6.fr

Abstract. Loss Differentiation Algorithms (LDA) are currently used to determine the cause of packet losses with an aim of improving TCP performance over wireless networks. In this work, we propose a cross-layer solution based on two LDA in order to classify the loss origin on an 802.11 link and then to react consequently. The first LDA scheme, acting at the MAC layer, allows differentiating losses due to signal failure caused by displacement or by noise from other loss types. Moreover, in case of signal failure, it adapts the behavior of the MAC layer to avoid a costly end-to-end TCP resolution. The objective of the second LDA scheme, which acts at the TCP layer, is to distinguish a loss due to interferences from those due to congestions and to adapt consequently the TCP behavior. The efficiency of each LDA scheme and of the whole cross-layer solution are then demonstrated through simulations.

1 Introduction

Due to various and unpredictable reasons (low noise immunity, overhead, throughput related to the distance…), the performance of TCP in the 802.11 [1] networks are not always as sufficient as the current applications require, particularly in SOHO (Small Office Home Office) environments or in public points of distribution (Hot Spot) with a wireless last link. In order to enhance elastic traffic performance in WLANs, several solutions have been proposed during the last few years (see section 2). Most of these proposals deal only with one layer (TCP or MAC) and they are either not adapted to 802.11 networks or require important changes in the current standard. Therefore, in an attempt to propose a solution that is compliant with the 802.11 standard, we suggest a cross-layer approach acting in a coordinated way on the two distinct MAC and TCP resolution levels. To do so, we propose two complementary Loss Differentiation Algorithms (LDA):

– The first one, implemented at the MAC layer, is used to identify losses due to wireless link failures that occur when the distance between the wireless station and its Access Point (AP) increases or when obstacles appear temporarily between them.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 297 – 309, 2006.

In this situation, the MAC *Retry Limit* parameter is dynamically adapted in order to maintain MAC retransmissions and thus to avoid a complete TCP resolution.

– The second LDA acts at TCP level and its objective, complementary to the MAC-level one, is to distinguish packet losses due to congestions from those related to short and repetitive signal losses due to interferences caused by other close transmissions in the same frequency band. This differentiation is realized through the monitoring of MAC level parameters. The integration of this second LDA scheme to the TCP *NewReno* process permits to avoid triggering the TCP loss recovery mechanism and reducing the TCP congestion window inadequately.

Hence, a cross-layer solution based on the combined use of both LDA schemes will allow to classify efficiently the three different loss causes (congestions, signal losses and interferences) and to react accordingly either at the MAC or TCP level.

The rest of this paper is organized as follows: section 2 presents a brief analysis of the various approaches proposed in the literature to improve TCP in WLANs. In section 3, the MAC-layer LDA and the associated adaptation are described and evaluated. Section 4 presents and evaluates the cross-layer LDA and the related TCP improvements. A summary of the loss cases and the associated differentiations are given in section 5; this later also shows the effectiveness of the whole cross-layer solution. Finally, section 6 concludes the paper and proposes some future issues.

2 TCP Improvements in WLANs

The TCP performance improvement attempts in wireless networks can be classified into three categories, according to the concerned layer within the protocol stack.

The first category concerns data link layer with two different proposed mechanisms. The first one is the improved *Logical-Link Control* (LLC) algorithm [3] which proposes to introduce queuing capabilities to the LLC sub-layer in order to delay frame transmission during signal losses. This algorithm gives very interesting results, but it requires important updates of AP and station firmware in order to establish and manage the added LLC queues. The second mechanism uses the *Automatic Repeat reQuest* (ARQ) protocol. It is demonstrated in [4] that ARQ improves TCP throughput. However, it is a specific data link layer protocol based on the retransmission requests of the lost frames and thus not easily adaptable to the 802.11 standard.

The second category of proposals concerns the transport layer and is based on the end-to-end resolution for existing TCP versions (Reno, Vegas…) [5-6]. These optimizations are made for the general context of wireless networks and thus do not give always good performance in 802.11 networks where a first level of error recovery is carried out at the MAC layer. Other end-to-end solutions use LDA [7-8] to differentiate loss types with successive measurements of *Round Trip Time* (*RTT*) or packet inter-arrival times. These algorithms are often efficient and easy to implement but they assume that TCP flows are relatively regular and that signal losses are unusual and not very persistent, which is not always the case when signal failure or interferences occur in WLAN.

The last category also concerns the transport layer but the control is made by a *Snoop Agent* located at the *Access Point* (AP). The *Snoop Agent* can manage two different mechanisms. The first one is the *Explicit Loss Notification* (ELN)

mechanism [9] in which the *Snoop Agent* is able to analyze all the transmitted segments and to set the ELN bit of the TCP header consequently. The agent installed at the AP operates at the TCP layer, which supposes a consequent modification of the firmware. In a second proposal [10], the *Snoop Agent* analyzes all the TCP segments in order to detect the duplicated acknowledgements and not to relay them in the event of signal loss. This permits to avoid alerting TCP and reducing the congestion window. In addition to the firmware modifications, this latter proposal requires a difficult adjustment between the different timeout involved in TCP, *Snoop* and MAC recovery mechanism.

Most of these proposals begin with the distinction between signal loss and TCP congestion. But the proposed solutions are not adapted to the 802.11 standard or require important modification of the firmware and are generally limited to a specific layer. From our point of view, an LDA-based solution, utilizing in a coordinated way the features of both concerned layers would give better performance. Moreover, we show that a distinction between TCP congestions and the two kinds of signal-losses, those due to mobility and those due to interferences, allows realizing a more efficient loss recovery in the targeted environment.

3 MAC-Layer LDA

A MAC-level retransmission occurs when the 802.11 acknowledgment is not received by the transmitter within the specified delay. For each retransmission, a counter is incremented until a threshold, named *Retry Limit*, is reached (default value is fixed to 6). Beyond this threshold, the frame is dropped.

For a connection using TCP, coherence between layers should lead to a fast MAC layer resolution (almost 1ms for a MAC timeout) before TCP is alerted when the segment loss is due to bad channel conditions. Otherwise, TCP will consider this packet loss as a congestion (almost 1s for a TCP timeout), which induces a reduction of the *congestion window* (*cwnd*) and a fall in the global throughput.

The measurements we carried out in [11] show that an increase of the *Retry Limit* value allows, for loss duration lower than the TCP *Retransmission TimeOut* (*RTO*), to recover the flow as soon as the channel is restored and thus provides a recovery mechanism faster than a standard TCP retransmission. We also showed that this mechanism is effective for signal loss of a few hundreds ms or more, typically caused by the displacement of the pedestrian user at the cover limit of its access point or by other pedestrians moving between the AP and the station. For shorter and repetitive signal losses caused by interferences, it is shown in [11] that a simple increase of the *Retry Limit* value does not improve the performance. Thus, we suggest treating these different types of losses differently.

3.1 Principle

As a systematic increase of the *Retry Limit* value can either be inadequate in some cases (congestion) or ineffective in some others (interferences), we suggest here the use of a *Loss Differentiation Algorithm*. The objective of this LDA is to know when this increase is appropriate and to realize a dynamic adaptation of *Retry Limit*

accordingly. Let us note that although the *Retry Limit* parameter is configured statically in all the implementations, it can be dynamically modified without contradicting the 802.11 standard.

To identify signal losses caused by the distance or obstacles, it is inappropriate to employ a Transport-layer LDA. Such schemes use successive values of *RTT* or packet inter-arrival times and it is not possible to make these measurements when the channel is unavailable (signal loss can be of a few hundreds ms or more). A more appropriate parameter for this differentiation is the *SNR* (*Signal to Noise Ratio*) given at the MAC layer.

In the MAC 802.11 frames, the "signal" field specifies the current throughput used to transmit the following data (*Data Rate*). This throughput indication depends on the measured power received by the station before its transmission and is thus proportional to the SNR. In addition, this throughput is related to the *Auto Rate Fallback* (ARF) procedure implemented by all the 802.11a, b or g card manufacturers. Let us recall that this procedure automatically reduces the throughput when a drop in the SNR is sensed. This can be due either to distance or obstacles.

The proposed LDA is based on the simple fact that if *SNR* (or *Data Rate*) is maximal, the probability that the segment loss is due to a signal failure caused by the distance and not to TCP congestion is very weak. In the mean time, this probability increases with the decrease of *SNR*. Thus, the idea of the proposed LDA is to allow a dynamic *Retry Limit* adaptation according to the *Data Rate* given at the MAC 802.11a, b or g layer. The algorithm depicted in Table 1 applies to the 802.11g standard where the throughput decreases gradually from 54Mbps to 6Mbps while passing by 24Mbps and 12Mbps. The increase of the *Retry Limit* threshold is linear and progressive (the default value of 6 is successively added) to avoid congesting the channel unnecessarily when this latter is used by other transmissions.

Note that the *Retry Limit* increase is bounded by three events:

– the arrival of the MAC acknowledgment for a retransmitted segment;
– the TCP transmission window is emptied;
– the RTO is reached without the channel being restored.

When one of these events occurs, the *Retry Limit* is reset to its initial value (i.e. for future transmissions). This help to avoid occupying the channel unnecessarily. In addition, one should note that, during the RL increase phase, the fairness with other

Table 1. MAC-layer LDA

```
if (DataRate ≥ 12Mbps) then          // station is closed to AP
    RetryLimit = 6                   // default value
else if (DataRate > 6Mbps)           // possible signal failure
    RetryLimit = 12                  // begin to enlarge transmission window
else if (DataRate ≤ 6Mbps)           // probability of failure is max
    RetryLimit = 18                  // continue to enlarge window
    if (new segment) && (last segment dropped)
                                     // new TCP segment and last MAC retry failed
        RetryLimit = RetryLimit + 6  // enlarge again window
    end if
end if.
```

MAC traffics on the same channel is preserved thanks to the 802.11 backoff algorithm which increases exponentially the time between two retransmissions according to the index of this latter. Also note that the others MAC traffics are not directly concerned by the *Retry Limit* increase because the *Data Rate* field transported in the frames is specific to each wireless station and its transmission conditions (distance, obstacles …)

3.2 Simulation Results

In order to analyze the performance improvements brought by the MAC-layer LDA, a set of simulations are carried out using NS-2 [12]. The 802.11 implementation already available within NS-2 have been extended in order to incorporate the more recent 802.11g specificities including the ARF procedure. The simulated network reproduces a usual SOHO environment with a wireless last hop interconnecting an 802.11 station receiving a FTP/TCP flow from a wired network. Signal losses are simulated by moving the wireless station out of the coverage area of its AP. The packet length is 1460Bytes, the default TCP retransmission timeout is 1s and the TCP version is NewReno, The choice of this TCP variant is motivated by the fact that it gives the best results in an access network with a wireless last hop [13].

Fig. 1 shows the evolution of the average throughput for the TCP flow during a signal loss according to its duration, with and without MAC-layer LDA. The average throughput is measured according to the number of TCP segments successfully transmitted during a 1s observation period starting at the beginning of the signal failure (this duration corresponds to the default TCP timeout). The loss duration interval is selected to have a dozen values between a short loss of few ms and *RTO*.

The maximum *Data Rate* of 4.6Mbps (*Signal Rate* of 6Mbps) is obtained, according to the ARF procedure, when the mobile is at the limit of the coverage area. The default values of the TCP window and *Retry Limit* are Win=8KB and RL=6. In this case, the MAC loss-recovery is not effective and the average throughput reaches the

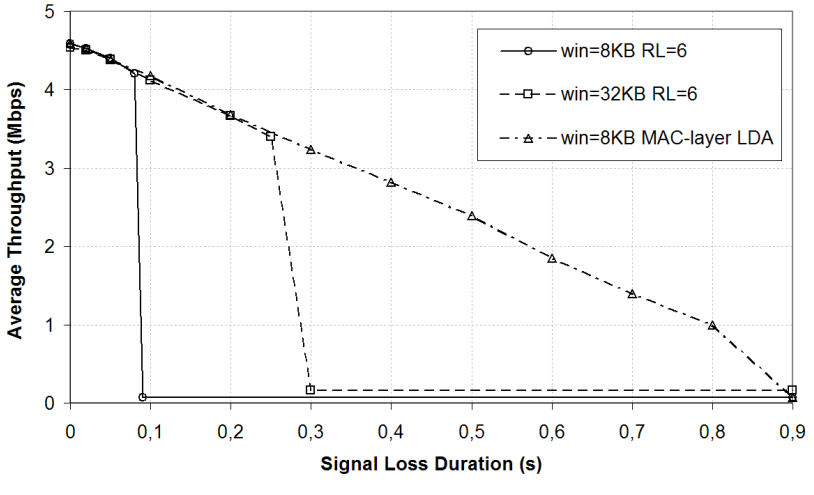


Fig. 1. TCP improvements with MAC-layer LDA

null value for loss duration of 0.1s or more. Fig. 1 also depicts that the increase of the TCP window size (Win=32KB) can improve the loss-recovery as well. However it leads to more end-to-end TCP retransmissions, which increases the delays. The last curve shows that the MAC-layer LDA and the dynamic *Retry Limit* adaptation can improve the performance significantly. In this case, the loss-recovery is effective for loss duration up to 0.8s, and the flow is maintained for all these cases allowing TCP to react immediately when the channel is restored rather then waiting for *RTO*.

4 Cross-Layer LDA

Since signal failures due to distance or obstacles are resolved by the MAC-layer LDA, the objective here is to differentiate segment losses due to interferences from those due to congestions.

4.1 The Proposed LDA Scheme

As proposed in the literature, the differentiation decision can be obtained based on TCP parameters, namely *RTT*, packets inter-arrival times and *congestion window* (*cwnd*). Our simulations with a wireless last hop show that the TCP variable presenting the most significant variations in the event of signal losses compared to congestions is the *RTT*. We thus selected three TCP-layer LDA schemes based on comparisons of current *RTT* values with different thresholds and on filters giving more or less weight to the recent samples: the *Vegas Predictor* scheme [14], the *Spike* scheme [7] and the *Flip Flop Filter* [15]. Then, rather than using only TCP-layer parameters which do not take into account the 802.11 specificities, we suggest to use a cross-layer approach as an alternative to conventional TCP-Layer LDA schemes. Even if the final objective of the algorithm is to indicate how to adjust the TCP behavior, the use of MAC-layer parameters to identify the cause of segment-losses can lead to a more accurate differentiation.

The idea of our alternative algorithm is to count the number of MAC retransmissions for each of the *n* segments composing the current TCP window when the TCP layer is alerted by the reception of three duplicated acknowledgements. As described in Table 2, if for one of these segments at least, the number of MAC retransmissions (*RetryCount*) is equal to the threshold (*Retry Limit*), we consider that the loss is due to interferences and not to TCP congestion. Indeed, in the case of congestion, the surplus

Table 2. Cross-layer LDA

```
if (3 dup ack) then                          // loss indication in TCP NewReno algo
    LDA_Estimator = 0                        // initial value for congestion
    for (i = 0 ; i ≤ n ; i ++)               // for all the not acknowledged segments
       if (RetryCount = RetryLimit) then     // segment is dropped, probably a short loss
           LDA_Estimator  = 1                // set value for interferences
       end if
    end for
end if.
```

of segments is eliminated from the queue of the concerned node and MAC retransmissions are theoretically not used; inversely, in case of persistent interferences, the segment is dropped by the MAC layer after reaching the *Retry Limit* threshold. This algorithm assumes that for all the not acknowledged TCP segments, the value of *RetryCount* is stored. The *ACKFailureCount* counter available in the 802.11 *Management Information Base* (MIB) [1] gives the number of times that an expected ACK is not received and consequently the value of *RetryCount*.

Note that while the TCP sender is not a wireless host and that the TCP flow is forwarded to the wireless receiver through an AP, an additional stage is necessary. The *LDA_Estimator* is first set at the AP's MAC layer. Then this latter informs the TCP sender by setting consequently the *ELN* (*Explicit Loss Notification*) bit of the TCP header in the ACK segments (i.e. *ELN=LDA_Estimator*=1 in case of interferences). The loss differentiation is finally made at the TCP sender when receiving three duplicated ACKs. This mechanism is inspired from the one used with the *Snoop Agent* described in section 2. However, our solution does not concern the whole TCP layer but only the *ELN* bit of the TCP header is affected. The modification of the AP's firmware here is minimal compared to the analysis of all the transmitted segments that is performed by the *Snoop Agent*.

In order to realize a comparative study among the 4 selected LDA schemes, a set of simulations targeting a wireless context with a last link undergoing congestions or interferences have been realized. The simulated network is the same one as for section 3. Interferences are caused by the transmission on the same channel of a CBR/UDP flow between two other wireless stations out of the AP coverage and interferences areas. As we deactivated the RTS/CTS mechanism for both transmissions, the AP will not detect CBR transmissions and will thus transmit its TCP segments towards the receiver which is located in the interference area. The duration and the frequency of the interferences will vary according to the size of the packets and the rate of the CBR source. A good compromise is found with packets of 1000Bytes and frequency interval starting from 900packets/s (denoted 0% in the curves) to 1800packets/s (denoted 100% in the curves). Indeed, for lower frequencies, the loss rate is not significant while for higher frequencies, the wireless link is completely saturated by the CBR source. Let us note that the simulated interferences and so the packets losses are carried out in a scenario close to reality (short losses are often caused by transmissions in the same frequency band) and not with a theoretical packet error rate as inaccurately used in most studies.

Another CBR/UDP flow is established between the server and a fourth wireless station in order to saturate the AP and induce congestions. For this flow, the compromise is found with packets of 1000Bytes sent with a frequency varying from 1600packets/s (denoted 0%) to 3500packets/s (denoted 100%). Note that only one CBR source is active at the same time, i.e. interference and congestion cases are analyzed separately for a better understanding of the obtained results.

The simulation results presented in Fig. 2 and Fig. 3 show the accuracy (the percentage of correctly classified losses) of the four LDA schemes according to the interference or congestion rate. For the *Vegas predictor* scheme, we observe that the losses due to low interference rates or high congestion rates are badly classified (less than 60%). This is especially due to the evolution of *cwnd,* which is in these cases inadequately used in conjunction with *RTT* to compute the *Vegas predictor*. The *Spike*

scheme, only based on *RTT* variations, gives slightly better results: accuracy higher than 80% in the majority of the cases. The badly classified losses are more random and are mainly due to the calculation mode of the Spike's thresholds. The *Flip Flop* filter is not very efficient, particularly for losses due to interferences. The used algorithm employs many parameters difficult to regulate. Finally, the proposed cross-layer LDA scheme gives the best results. For congestions, there are almost no MAC retransmissions and the *Retry Limit* threshold is never reached, which gives 100% of correctly classified losses. For interferences, some losses are badly classified when

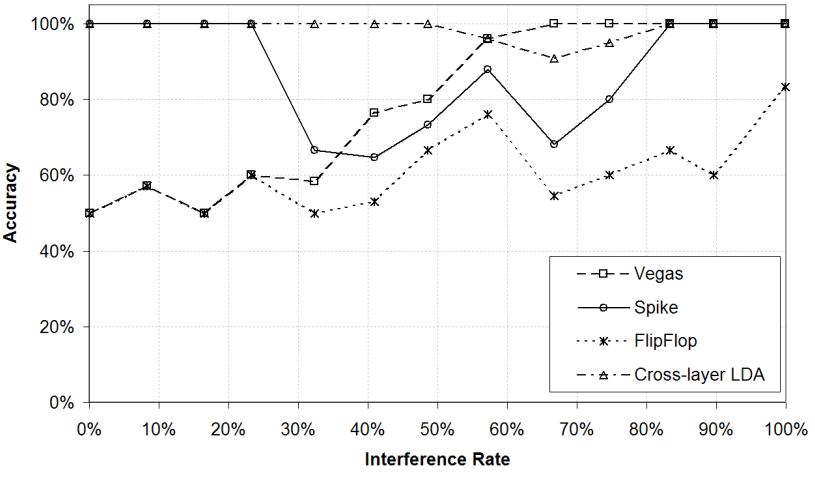


Fig. 2. Accuracy of the 4 LDA schemes with Interferences

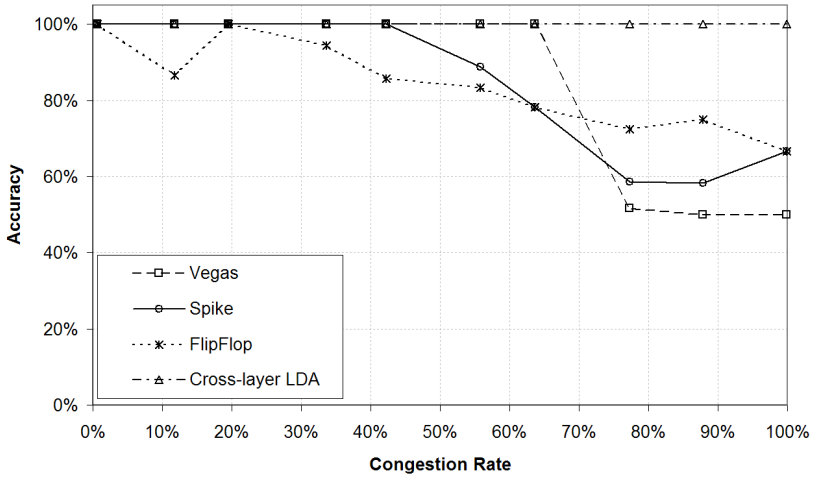


Fig. 3. Accuracy of the 4 LDA schemes with Congestions

the segment is finally received with the last attempt. However accuracy remains in all the cases higher than 90%. For the continuation of the study, we will thus use this scheme as the basis of the TCP behavior enhancement.

4.2 TCP NewReno Enhancement

When the source detects a segment loss, i.e. when 3 duplicate acknowledgements are received, the cross-layer LDA is asked to know the cause of the packet loss:

- If the loss is classified as due to congestion, a normal TCP *NewReno* reaction is triggered and *cwnd* is halved;
- If the loss is classified as due to interferences (short signal loss), *cwnd* is not reduced. This allows the source to achieve higher transmission rates in the event of short successive signal losses, if compared to the blind reduction of the throughput performed by the legacy operations of TCP.

This simple extension of the TCP *NewReno* algorithm with an LDA scheme was already proposed in other studies [15]. To this extension, we also added a second adaptation in order to treat the case where a loss due to interference is detected after *RTO*. When a segment-loss, classified as due to interference (i.e. when *LDA_Estimator*=1), is not solved quickly and that a TCP timeout is nevertheless triggered, the idea is to not increment the initial value of *RTO* (in almost all TCP variants, the *RTO* value is doubled after each loss detected through TCP timeout). The aim being to avoid slowing down the loss-recovery process for the following segments.

Simulations are carried out using the same scenarios as for the previous paragraph. Fig. 4 shows the evolution of the average throughput for the TCP flow during congestion or interference periods (the rates are tuned according to the frequencies of the corresponding CBR sources). The maximum *Data Rate* of 25Mbps (*Signal Rate* of

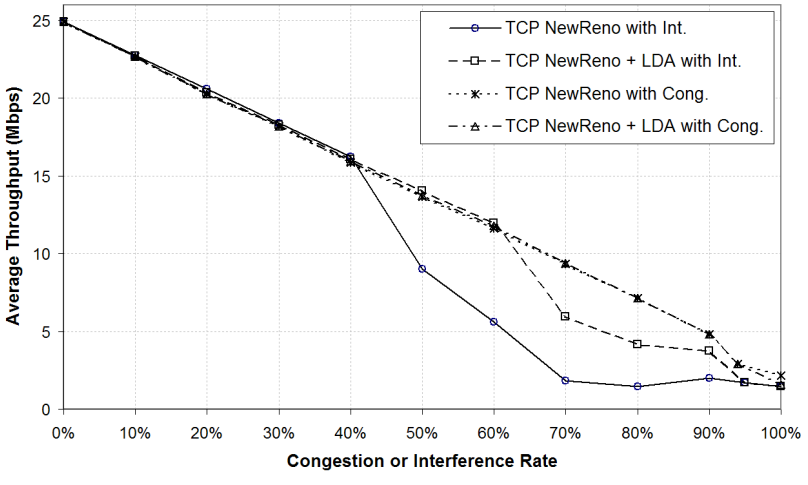


Fig. 4. TCP improvements with Cross-layer LDA

54Mbps) is obtained, according to the ARF procedure, when the station is quite close to its AP. Here, the station is static and the reduction of the throughput is only obtained by varying the rates of the CBR sources. The default values of the TCP window and *Retry Limit* are Win=32KB and RL=6.

In case of congestion, we verify that there are almost no changes with or without the LDA. Indeed in this situation, the TCP *NewReno* algorithm is not modified allowing this protocol to behave as fairly as the standard TCP protocol in event of congestion. This result confirms moreover the efficiency of the cross-layer scheme to identify congestions. In case of interferences, the throughput is clearly improved for interference rates higher than 40%. Indeed, when the number of duplicate acknowledgements increases (for interference ratio higher than 40%), the non reduction of *cwnd* limits the fall of the TCP throughput. Hence, the slight and linear decrease of the TCP throughput is maintained for interference rates up to 60%. For interference rates above 60%, the maintenance of *RTO* helps to limits the fall in performance and the TCP throughput is maintained.

5 Overview of Losses and Differentiations

Fig. 5 gives an outline of all segment-loss reasons on an 802.11 wireless link:

- The differentiation of cases 4 and 5 is carried out by the cross-layer LDA. In these cases, the TCP *NewReno* adaptation is in charge of improving the performance of elastic flows in the event of interferences (cf. paragraph 4.2).
- The MAC-layer LDA based on *SNR* is used to differentiate the cases 1, 2 and 3 from 4 and 5. For case 3, the *Retry Limit* adaptation is used to improve the performance significantly (cf. paragraph 3.1). Note however that when the station is

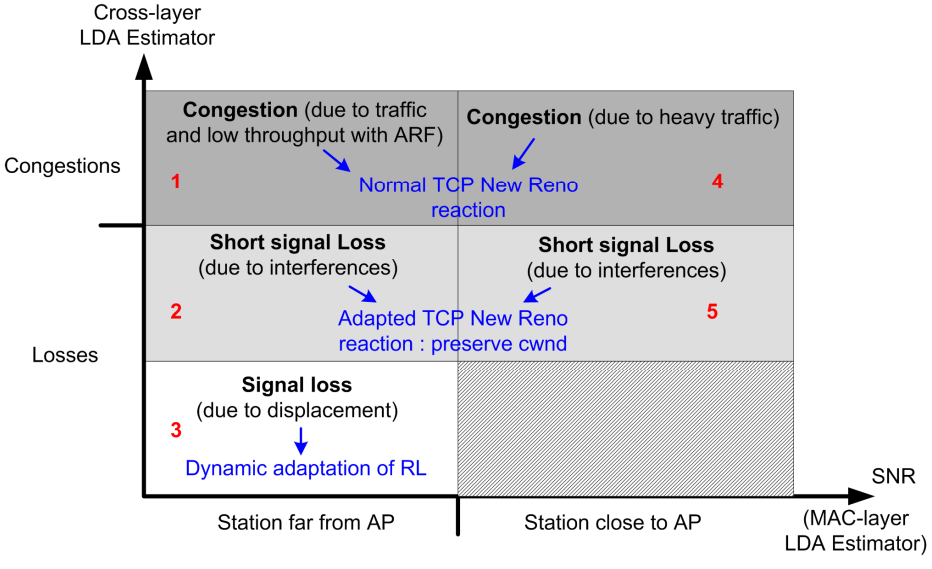


Fig. 5. Loss-recovery for different loss cases

far away from its AP, the differentiation algorithms do not make possible the distinction between case 3 from the cases 1 and 2. Remember that case 1 is distinguished from case 2 by the cross-layer LDA.

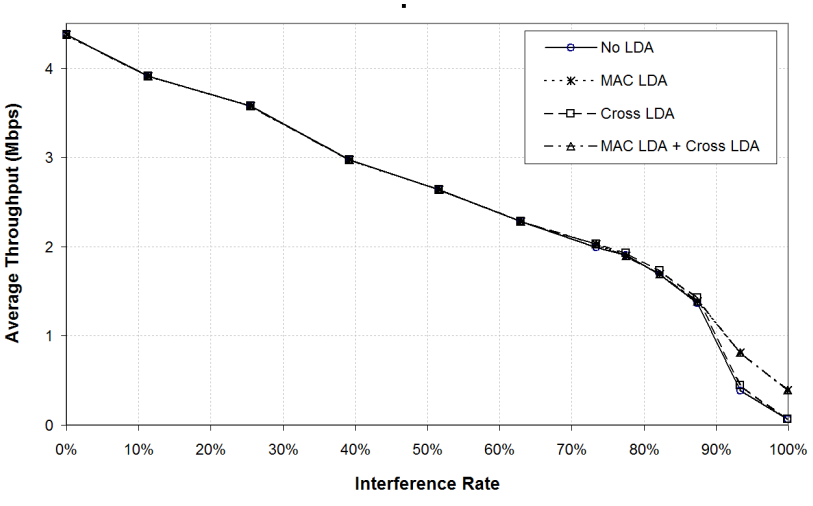


Fig. 6. TCP performance with low throughput (low SNR) in case of interferences

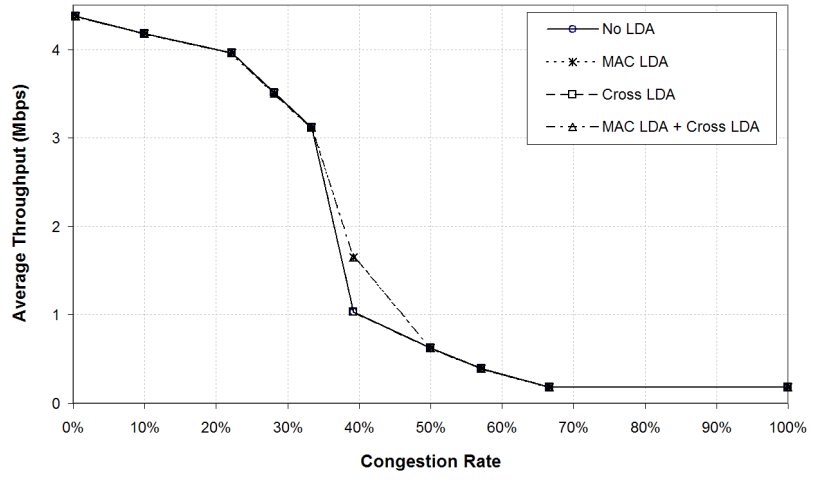


Fig. 7. TCP performance with low throughput (low SNR) in case of congestions

Hence, segment-losses due to distance can not be clearly differentiated from those due to interferences when the *Signal Rate* is reduced to 6Mbps. This is however not constraining. Fig. 6 shows that the evolution of the TCP throughput, when the *Signal Rate* is reduced to 6Mbps, is slightly influenced by the intervention of one or the other LDA. Note however that the use of the MAC-layer LDA gives better improvements compared to the use of the cross-layer LDA. This is more clearly verified for interfer-

ence rates above 85%. Indeed, for these interference rates, we have an increase of the MAC retransmissions which limits the number of segment-losses and thus avoids triggering TCP congestion control algorithms. With a reduced *Signal Rate*, the effects of this improvement on the data throughput remain nevertheless limited. Note also that when both proposed LDA schemes are used in conjunction (MAC LDA + cross-layer LDA), the MAC-layer LDA intervention is happening firstly. Finally, Fig. 7 shows that the evolution of the TCP throughput according to the congestion rate is not significantly influenced by the corrections introduced by both LDA schemes. Indeed, in this case a normal TCP reaction is triggered which corresponds to what should be completed. These results thus show the uselessness of a new LDA scheme to distinguish case 3 from cases 1 and 2.

6 Conclusion

According to the characteristics of the various loss causes (mobility and obstacles, interferences caused by other transmissions in the same frequency band and congestion due to increased traffic conditions), we proposed in this paper two Loss Differentiation Algorithms acting respectively at the MAC and TCP layers and both using MAC layer parameters. Depending on the operations of these LDA, adaptations of the MAC and TCP recovery mechanisms are then proposed. The performance evaluation realized with a wireless network close to real situations have highlighted an improvement of the TCP flow performance in all cases. Hence we demonstrated: (i) the gain in performance due to the use of the MAC-layer LDA to react to signal-loss due to mobility and obstacles, and (ii) the efficiency of the cross-layer LDA to distinguish congestions from short losses due to interferences, thus allowing the effective improvement of the TCP behavior.

We are currently working on the optimization of the MAC-layer LDA. Actually, a default value of 6 is used in each RL increase stage. One possible optimization is to use a non-static value for realizing this increase. This value can be derived analytically depending on both TCP and MAC layer parameters.

References

1. IEEE 802.11 WG, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Standard, IEEE, 1999.
2. IEEE 802.11g WG, Part 11-Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 2003.
3. M. Bottigliengo, C. Casetti, C.-F. Chiasserini, M. Meo "*Short-term Fairness for TCP Flows in 802.11b WLANs*", IEEE INFOCOM 2004, Hong Kong, March 7-11, 2004.
4. A. Chockalingam, M. Zorzi, V. Tralli "*Wireless TCP performance with link layer FEC/ARQ*", IEEE ICC 1999
5. S. Mascolo, M.Y. Sanadidi, C. Casetti, M. Gerla, and R. Wang, "*TCP Westwood: End-to-End Congestion Control for Wired/Wireless Networks*" Wireless Networks J., 2002.
6. K. Xu, Y. Tian, and N. Ansari, "*TCP-Jersey for Wireless IP Communications*", IEEE JSAC, May 2004.

7. S. Cen, P. C. Cosman, and G. M. Voelker "*End-to-End differentiation of congestion and wireless losses*", IEEE/ACM Transactions on Networking (TON), 2003.
8. S. Bregni, D. Caratti, F. Martignon "*Enhanced Loss Differentiation Algorithms for Use in TCP Sources over Heterogeneous Wireless Networks*", Globecom 2003.
9. H. Balakrishnan and R. H. Katz "*Explicit Loss Notification and Wireless Web Performance*", Proc. IEEE Globecom, 1998.
10. C. H. Ng, J. Chow, and L. Trajkovic "*Performance Evaluation of TCP over WLAN 802.11 with the Snoop Performance Enhancing Proxy*", Opnetwork 2002.
11. S. Lohier, Y.Ghamri Doudane, G. Pujolle "*The Benefits of a Cross-Layer Approach for TCP Performance Improvements in WLANs*" , Proc. IEEE ASWN 2005.
12. The Network Simulator - NS-2, http://www.isi.edu/nsnam/ns/.
13. Q. Ni, T. Turletti and W. Fu. "*Simulation-based Analysis of TCP Behavior over Hybrid Wireless & Wired Networks*", WWIC 2002.
14. S. Biaz and N. H. Vaidya, "Distinguishing Congestion Losses from Wireless Transmission Losses: a Negative Result", Proc. of IEEE 7th Int.Conf. on Computer.
15. D. Barman and I. Matta, "Effectiveness of Loss Labeling in Improving TCP Performance in Wired/Wireless Networks", Boston University Technical Report, 2002.

Performance Evaluation of AQM Schemes in Rate-Varying 3G Links*

Juan J. Alcaraz and Fernando Cerdan

Department of Information Technologies and Communications,
Polytechnic University of Cartagena, Plaza del Hospital, 1, 30202 Cartagena, Spain
{juan.alcaraz, fernando.cerdan}@upct.es

Abstract. When TCP is carried over 3G links, overbuffering and buffer overflow at the RLC layer degrades its performance. AQM techniques at the RLC buffer can bring noticeable enhancements to TCP performance without introducing changes in 3G specifications. We show that the optimum parameter setting of AQM algorithms in RLC buffers is strongly related to the radio bearer rate, which can be changed dynamically by control layer protocols. By means of extensive simulation experiments we propose, for each specified nominal rate, optimum configurations that keep the goodput near the maximum while the delay is reduced up to 50%. We consider two AQM schemes, an adapted RED algorithm and a novel deterministic one, SBD described in this paper. We illustrate how an automatic reconfiguration of AQM parameters avoids the degradation caused by sudden changes in the radio bearer rate.

1 Introduction

Third generation cellular networks (3G) are expected to be an important part of the Internet. Many Internet applications like e-mail, web surfing and file transfer rely on TCP for the end-to-end transport. In 3G radio access networks, the link layer is managed by the Radio Link Control (RLC) protocol [1] which can be configured to provide a reliable service, recovering from propagation errors. A reliable RLC layer reduces packet losses perceived at TCP layer, avoiding the triggering of unnecessary congestion control measures [2, 3]. However, several characteristics of 3G links like high and variable latency and buffer overflow of the downlink buffers [4, 5, 6], have undesired effects on TCP performance.

In order to overcome these effects, recent works [5, 6] propose the application of Active Queue Management (AQM) techniques at the downlink RLC buffers. AQM can improve TCP performance over 3G links with a small change at the Radio Network Controller (RNC) nodes. In contrast to other proposals, this approach does not require changes in TCP itself and does not break the end-to-end semantics of TCP.

This paper addresses the configuration of AQM parameters in an RLC buffer considering the variations on the RB nominal rate. These variations have a significant effect on TCP performance, as we illustrate, and may be caused, e.g. by the 3G

* This work was supported by the Spanish Inter-Ministerial Sciece and Technology Commission under project TEC2005-08068-C04-01/TCM.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 310 – 321, 2006.

scheduling mechanisms or handovers among cells. We propose two alternative AQM schemes, Random Early Detection [7] (RED) and Slope Based Discard (SBD).

RED is one of the most extended AQM mechanisms for Internet routers, and its adaptation to the particularities of 3G links is described in [6]. We contribute providing further insight into the parameter setting of RED in radio bearers. Based of extensive simulation experiments we evaluate multiple RED configurations in different RBs.

SBD is a novel deterministic AQM algorithm especially suitable to the characteristics of 3G links. In this paper we describe SBD and disclose how its parameters should be configured regarding the RB bandwidth.

In the 3G protocol stack, the Radio Resource Control (RRC) protocol handles the resource management algorithms, setting up and modifying layer 1 and layer 2 protocol entities [8]. The operating scheme that we propose is completely compatible with this architecture: the RRC entity, responsible of changing the RB rate, should reconfigure AQM parameters according to the rate value. In this paper we provide examples of AQM reconfiguration under abrupt RB bandwidth changes. It should be noticed that these schemes do not require additional signalling because they operate only on the RNC side, and therefore could be implemented without introducing changes in 3GPP specifications.

The rest of the paper is organized as follows. Section 2 describes how a rate-varying RB degrades TCP performance. Section 3 explains the SBD algorithm in detail. Section 4 provides a brief description of the simulation environment and the simulation scenarios. Section 5 summarizes the parameter configuration guidelines for SBD and RED derived from the simulation results. Section 6 shows the operation of each algorithm under rate variations. The paper concludes in section 7.

2 Characteristics of 3G Links

Previous works [5, 9, 10] provide a clear view of the characteristics of 3G wireless links. Radio bearers are expected to multiplex a number of simultaneous connections ranging from 1 to 4 TCP flows [5, 11], because 3G links employs per-user buffering. At the RLC layer, the upper layer packets will be stored in the downlink buffer until they are fully acknowledged by the receiver side. In consequence, as described in [4, 10] frame losses in the downlink channel result in higher RLC buffer occupancy at the network side. Considering that the current RLC specification [1] proposes a drop-tail buffer, the buffer may overflow causing consecutive packet losses. This situation is especially harmful in the first stages of a TCP connection (slow start) and has a higher impact in TCP Reno, which can only recover from consecutive losses with a Retransmission TimeOut (RTO), causing the highest reduction of the rate.

The buffer should be large enough to avoid frequent overflow. However, excessive queuing cause some additional problems [4, 5] like Round Trip Time (RTT) inflation, unfairness between competing flows and viscous web surfing.

Fig. 1 illustrates the end-to-end goodput and delay of TCP over an RB for different RLC buffer sizes and a number of flows ranging from 1 to 4. The goodput represents the successfully received packets at the receiver and the delay is the transfer time of a packet in the downlink direction, at the TCP layer. The buffer size is given in RLC

Service Data Units (SDU) of 1500 bytes. Table 1 shows the parameter configuration for the RLC and TCP protocols. The RLC parameters were set according to the optimizing considerations described in [6, 9]. Further details on the simulator are provided in Section 4. As expected, Fig. 1 reveals that a larger buffer benefits the goodput performance but the overbuffering increases the latency.

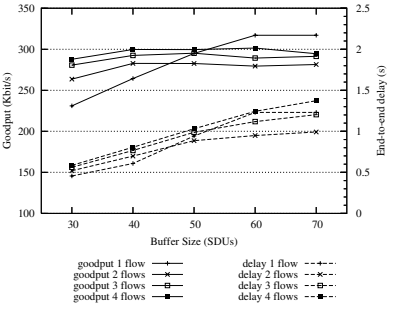


Fig. 1. TCP performance over a 384 kbit/s RB, with drop tail operation at RLC

Table 1. Simulation parameters

3G link parameters	Setting
PDU payload size	320 bits
TTI (Transm. Time Interval)	10 ms
Transmission window	1024 PDUs
maxDAT	10
In-order-delivery	true
Status Prohibit Timer	60 ms
Missing PDU detection	true
Poll Timer	60 ms
Wireless Round Trip Delay	50 ms
Normalized doppler frequency	0,01
Poll window	50 %
Last PDU in buffer Poll	yes
Last retransmitted PDU Poll	yes
Frame Error Ratio (FER)	10%

TCP parameters	Setting
Maximum TCP/IP packet size	1500 bytes
Maximum allowed window	64 kbytes
Initial window	1
Wired Network Round Trip Delay	200 ms

The rate variation of the RB may have additional effects on TCP performance. Fig. 2 shows the trace of two TCP connections over an RB which rate starts at 384 kbit/s and switches to 128 kbit/s 50 seconds after the start time. The curve at the top shows the RLC buffer occupancy (*BO*). The buffer capacity is set to 40 SDUs. The TCP congestion windows of each flow (*cwnd 1* and *cwnd 2*) are depicted below the *BO* curve, and the two curves at the bottom show, for each TCP flow, the sequence number of the packets when they are sent, received and dropped.

At the first stages of the connection, multiple packets are dropped due to buffer overflow, causing an RTO in both sources. The congestion windows shrink and the sources begin to recover their rate slowly. The overbuffering appears again, causing high delay and higher probability of additional overflows. At $t = 50$ the buffer overflows again because of the RB rate reduction. With a lower bandwidth in the 3G link, the overbuffering increases the latency even more and causes RTO inflation.

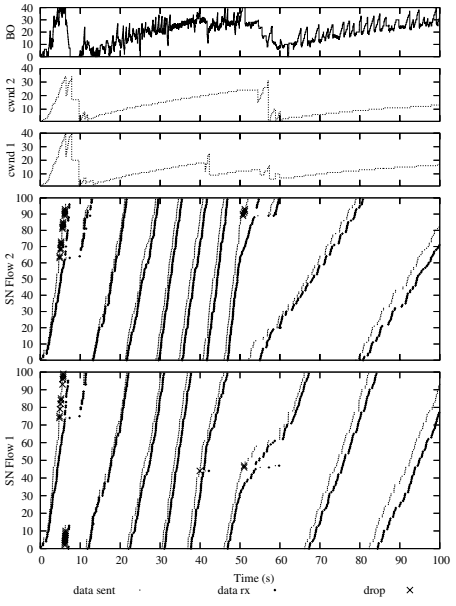


Fig. 2. Trace of two TCP connections carried over RLC

Given the behaviour of the buffer occupancy process in RLC, AQM techniques can be considered as a feasible strategy to enhance TCP performance over 3G links. AQM is aimed to maintain the buffer occupancy around a certain level, thus avoiding consecutive packet losses and reducing the delay jitter.

It should be mentioned that although RED is extensively used for Internet routers, its implementation in wireless link layer buffers is relatively novel. Thus, the effect of its parameter configuration on TCP performance is still not fully known. According to [5, 6], an RED algorithm at RLC should use the instantaneous queue size to react faster to sudden *BO* increments and to reduce operational complexity.

3 Slope Based Discard

We propose a novel AQM algorithm for the downlink RLC buffer in 3G networks, named Slope Based Discard (SBD).

The SBD algorithm is based on the following ideas:

1. A packet discard is a congestion signal directed to the TCP sender side that takes a certain amount of time, T_S, to arrive at the TCP source (see Fig. 3). The rate reduction is perceived at the buffer after the propagation time, T_f, of the fixed (wired) network.
2. The discarding policy is driven by the buffer filling rate, r. In normal operation, whenever r exceeds a critical value, r_c a packet is dropped. The buffer occupancy level determines the value of r_c.
3. r_c represents the filling rate that, if sustained, would fill the buffer entirely before the rate reduction can be perceived at the buffer after a packet discard.

4. After a packet drop, additional packet discarding should be avoided until the rate reduction at the TCP source can be noticed at the RLC buffer. In Fig. 3 this reaction time equals $T_S + T_f$.
5. The packet chosen for discard will be as close as possible to the front of the queue, in order to reduce the reaction time. Additionally, the algorithm should not discard a packet if its transmission over the RLC link has already started. Otherwise, upon a packet discard, the RLC would start the signalling procedure required to synchronize RLC sender and receiver sides [1]. Consequently, our protocol discards the first packet whose transmission has not started, thus reducing complexity and avoiding changes in the 3GPP specification itself

The following parameters control the SBD algorithm:

- *minth*: buffer occupancy level above which packets can be dropped.
- *maxth*: maximum occupancy allowed in the buffer.
- T_r: estimated reaction time.
- α: occupancy interval used for the estimation of the slope of *BO* process curve.

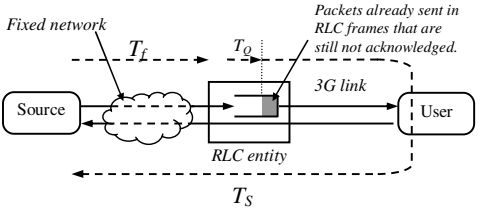


Fig. 3. Schematic diagram of the end-to-end connection with the delay times of each section

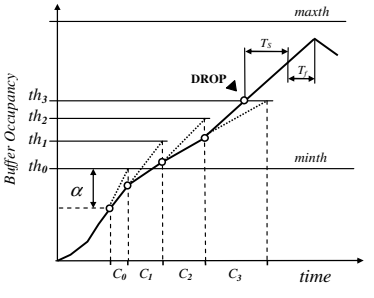


Fig. 4. Buffer ccupancy curve of a buffer implementing SBD

Fig. 4 depicts the buffer occupancy (*BO*) process in an RLC buffer as a graphical example of the algorithm.

When *BO* is higher or equal to $minth - \alpha$, the algorithm calculates the time C_n that it will take the buffer to store α additional bits at a filling rate equal to r_c ($C_n = \alpha / r_c$). The threshold level for the measuring interval is also determined ($th_n = BO + \alpha$). The value of r_c depends linearly on th_n according to the definition and expressed in (1).

$$r_c = \frac{maxth - th_n}{T_r} \tag{1}$$

A timer for C_n is started. If the timer expires and *BO* is below the threshold th_n, then the actual filling rate is lower than r_c, and no packet is dropped. If th_n is reached before the expiration of the timer, the current filling rate surpasses r_c and therefore a packet will be discarded.

In Fig. 4, the dotted segments starting at each measuring interval represent the buffer filling at the critical rate (critical curve). In the intervals C_0, C_1 and C_2, no packet is discarded because the *BO* curve is below the critical curve. In contrast, in

the C_3 period, *BO* is above r_c. Hence, the threshold th_3 is reached before the timer C_3 expires. When th_3 is reached, a packet is dropped. The monitoring and discarding algorithm is deactivated for a period T_r, avoiding consecutive packet discards. The following pseudocode summarizes the algorithm operation.

Pseudocode of the SBD operation.

```
for each packet arrival
  update BO
  if timer C_n on
    if BO ≥ th_n
      drop packet
      deactivate timer C_n
      start timer T_r
  if timer C_n off
    if (BO ≥ minth - α)
      calculate C_n
      th_n = BO + α
      start timer C_n

upon timer (C_n or T_r) expiration
  if (BO ≥ minth - α)
    calculate C_n
    th_n = BO + α
    start timer C_n
```

One of the main advantages of SBD compared to random or RED-like mechanisms is that it does not need to generate random numbers to compute the discarding probability because of its deterministic operation. This reduces the computational cost of the algorithm, and makes it more feasible for its implementation at the RLC level where the buffering is done in a per-user basis.

The maintenance of a new timer, C_n, does not add too much complexity to the RLC operation, which already handles several timers, e.g. *Poll Timer* and *Status Prohibit Timer* [1]. The RLC can synchronize C_n to the Transmission Time Interval (TTI) which is equivalent to a clock signal with a granularity of 10 ms (similar to that of other RLC timers).

4 Simulation Environment

The simulation environment employed in this research has been developed in OMNeT++ [12] and comprises a complete implementation of TCP and RLC protocols. Similar simulators were described in [9, 10]. The simulation topology, shown in Fig. 5 consists of one or several TCP sources connected to their respective receivers in the user's equipment (UE). The end-to-end connection consists of two sections, the wired network and the radio bearer. The wired network comprises the Internet and the 3G core network. The radio bearer has a round trip time (RTT_w) of 50 ms [2, 8] and a bidirectional nominal rate ranging from 384 kbit/s to 64 kbit/s, representing the bottleneck link, which is the situation expected in most cases [11]. The wired (fixed) network is modeled with a 1 Mb/s link with a round trip delay (RTT_f) of 200 ms [2].

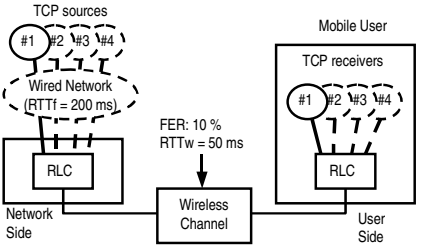


Fig. 5. Schematic representation of the simulation environment

The wireless channel generates error bursts according to the model described in [13] where the Doppler frequency, f_d, of the UE determines the average burst length. Lower f_d causes longer bursts of errors. It is usual to employ the normalized Doppler frequency, equal to the product of f_d and the radio frame duration (10 ms).

In order to obtain more realistic results, the error probability in our model is the same in the uplink and in the downlink direction. The frame loss ratio is 10%, a typical UMTS design value [2, 8].

The simulation results exposed in this paper are obtained averaging 20 runs per sample and the radius of each confidence interval is estimeated with a confidence degree of 90% according to a t-student distribution.

The TCP flavour employed is TCP Reno, one of the most extended in the Internet [11]. RLC and TCP parameter setting is shown in Table 1.

5 Parameter Configuration

In our simulations, multiple parameter combinations of RED and SBD were tested, in order to disclose the effect of each one on the end-to-end performance. Four standard RB rates are considered: 384, 256, 128 and 64 kbit/s.

In both SBD and RED the following values of *minth* were evaluated: 5, 10, 15, 20, 25 and 30 SDUs. The value of *maxth* equals the size of the RLC buffer, 40 SDUs, enough to prevent buffer overflow, keeping a low delay. In SBD the values of T_r ranged from 50 ms to 5000 ms, and α is equal to 5 SDUs, which was found to be an optimum value and a compromise value between fast detection of congestion and excessive sensitivity to occupancy oscillations.

Figures 6 and 7 show the average goodput and delay of 1 and 4 TCP connections over a 384 kbit/s RB for different combinations of SBD parameter values. Figures 8 and 9 show the performance figures for a 128 kbit/s RB.

The following conclusions are derived regarding each parameter:

1) T_r has a direct impact on the aggressiveness of the discarding policy. According to (1), a higher T_r reduces r_c, and thus, the delay decreases.

2) minth determines a lower bound for the goodput and the delay because it sets the minimum TCP *cwnd* to allow a packet discard. To avoid link underutilization, *minth* should be above the Bandwidth Delay Product (DBP) of the connection, defined as the product of the Round Trip Propagation Delay (RTPD = RTT_w + RTT_f) with the

bottleneck link rate. Our results show that *minth* should be set, at least, to 2×BDP in order to maintain the goodput near the optimum for a wide range of T_r values.

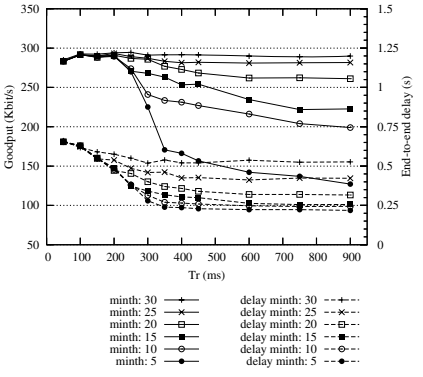


Fig. 6. Performance of one TCP flow over a 384 kbit/s radio bearer with SBD

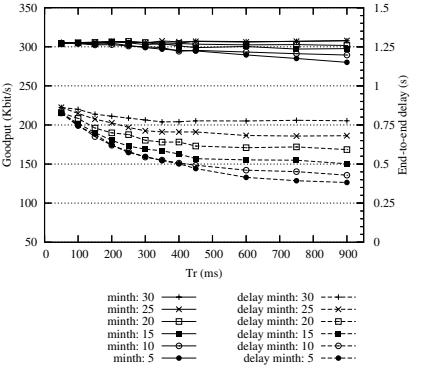


Fig. 7. Performance of 4 TCP flows over a 384 kbit/s radio bearer with SBD

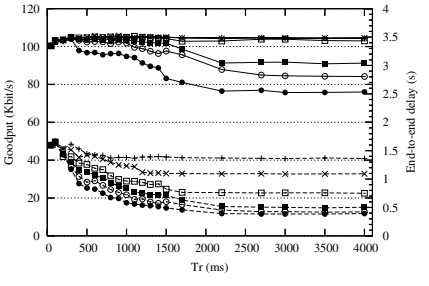


Fig. 8. Performance of one TCP flow over a 128 kbit/s radio bearer with SBD (see call-outs in Fig. 6)

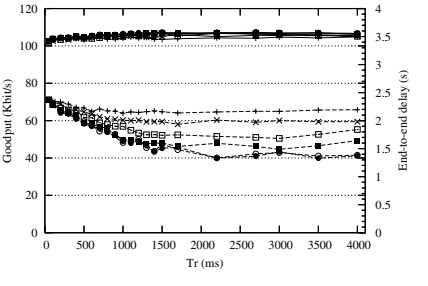


Fig. 9. Performance of 4 TCP flows over a 128 kbit/s radio bearer with SBD (see callouts in Fig. 7)

Comparing the performance for one and several TCP flows, we conclude that the optimum parameter setting for each nominal rate should be determined for the single TCP flow scenario. In this case, the goodput decays when the discarding policy is too aggressive (high T_r values and/or low *minth*). This fact is easily explained considering TCP *cwnd* dynamics. Using AQM, an early packet discard halves the window of the TCP connection. Obviously, in a single flow scenario this measure halves the overall user rate. This avoids buffer overflow but limits the goodput improvement. In a multiple flow scenario the overall user rate reduction is less severe because it only affects one connection upon each packet discard.

The maximum achievable goodput values with SBD, shown in Table 2, are tied to high delays. Considering these performance values as a reference, a more aggressive setting of *minth* and T_r can lead to a delay reduction of up to 30% with a negligible reduction of the goodput (between 1% and 4%), as shown in Table 3.

Table 2. Maximum average goodput values in SBD simulations for the single flow case

RB	T_r (ms)	*minth* (SDUs)	Goodput (kbit/s)	Delay (s)
384	250	30	294.5 ±5.6	0.55 ± 0.02
256	300	25	203.6 ± 3.6	0.71 ± 0.02
128	900	20	105.0 ± 1.6	0.99 ± 0.04
64	1500	10	52.5 ± 0.8	1.97 ± 0.14

Table 3. Proposed SBD configuration and its performance values in the single flow scenario

RB	T_r (ms)	*minth* (SDUs)	Goodput (kbit/s)	Delay (s)
384	200	20	290.5 ± 4.2	0.47 ± 0.03
256	500	20	200.1 ± 3.7	0.53 ± 0.02
128	1300	15	102.1 ± 1.5	0.72 ± 0.03
64	2500	10	50.4 ± 1.5	1.12 ± 0.12

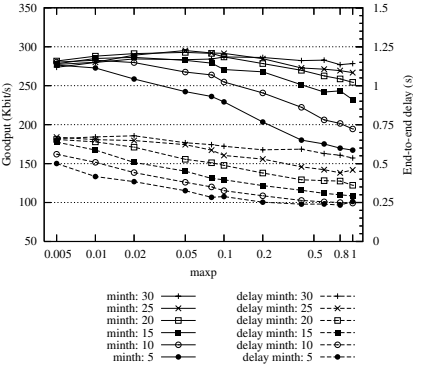


Fig. 10. Performance of one TCP flow over a 384 kbit/s radio bearer with RED

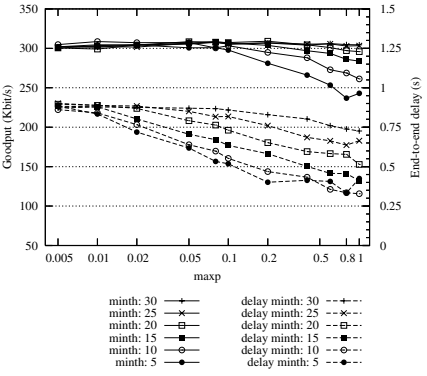


Fig. 11. Performance of 4 TCP flows over a 384 kbit/s radio bearer with RED

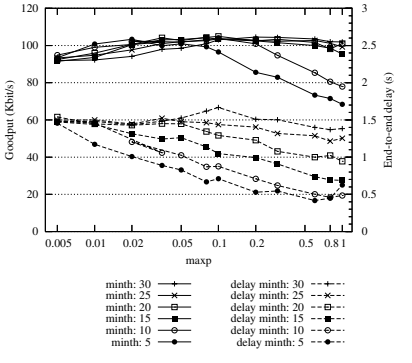


Fig. 12. Performance of one TCP flow over a 128 kbit/s radio bearer with RED

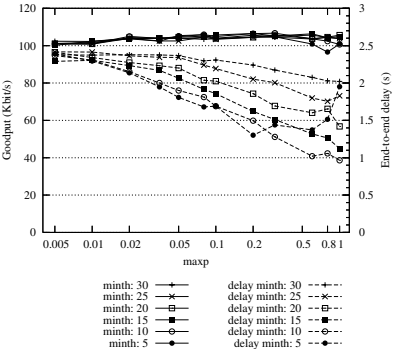


Fig. 13. Performance of 4 TCP flows over a 128 kbit/s radio bearer with RED

In the simulations of the RED schemes, the values of *maxp* ranged from 0.005 to 1. Figures 10 and 11 show the average goodput and delay of 1 and 4 TCP connections over a 384 kbit/s RB, and Figures 12 and 13 show the performance figures for a 128 kbit/s RB. As expected, the single flow scenario is more responsive to RED parameter changes, and therefore it is the worst case for configuration.

Following the same criteria used in SBD, the maximum goodput values, shown in Table 4, are taken as a reference to select parameters with a better balance between goodput and delay performance. The proposal is shown in Table 5.

Table 4. Maximum average goodput values in RED simulations for the single flow case

RB	*maxp*	*minth* (SDUs)	Goodput (kbit/s)	Delay (s)
384	0.05	25	295.1 ± 5.9	0.62 ± 0.02
256	0.08	20	204.5 ± 3.6	0.75 ± 0.03
128	0.1	10	103.8 ± 1.3	0.88 ± 0.03
64	0.1	10	52.3 ± 0.9	1.57 ± 0.08

Table 5. Proposed RED configuration and its performance values in the single flow scenario

RB	*maxp*	*minth* (SDUs)	Goodput (kbit/s)	Delay (s)
384	0.05	20	292.7 ± 4.6	0.52 ± 0.02
256	0.06	15	203.3 ± 2.4	0.63 ± 0.02
128	0.2	10	100.9 ± 1.8	0.70 ± 0.03
64	0.3	10	50.0 ± 1.9	1.32 ± 0.14

Table 6. Performance of a drop-tail buffer and the relative improvement of SBD and RED

RB	Flows	Goodput (kbit/s)	SBD	RED	Delay (s)	SBD	RED
384	1	277.1 ± 6.1	+5%	+6%	0.72 ± 0.04	–34%	–27%
	4	298.6 ± 4.8	+3%	+3%	0.89 ± 0.01	–21%	–21%
256	1	185.1 ± 4.5	+8%	+10%	0.94 ± 0.07	–43%	–32%
	4	201.9 ± 3.1	+4%	+2%	1.28 ± 0.02	–25%	–19%
128	1	89.9 ± 5.8	+14%	+12%	1.58 ± 0.14	–54%	–55%
	4	93.4 ± 2.6	+8%	+7%	2.44 ± 0.06	–35%	–39%
64	1	42.1 ± 1.4	+20%	+19%	3.12 ± 0.21	–64%	–58%
	4	48.5 ± 1.6	+8%	+8%	4.33 ± 0.09	–23%	–40%

Finally, Table 6 shows the performance of a drop-tail buffer and the improvement achieved by the proposed SBD and RED configurations. While both schemes are similar in terms of goodput improvement, SBD tends to achieve greater delay reductions than RED, especially for the single flow case. Besides, SBD configuration is somewhat easier than RED because the delay is directly reduced increasing T_r (could be tied to application requirements), while *minth* acts as a "security" limit, assuring that the goodput does not fall below certain value.

6 Operation in Rate-Varying 3G Links

In this section we show how an RLC buffer with automatic AQM reconfiguration reacts to a sudden change in the RB rate. The chosen example consists of two TCP flows served by a 3G link that starts at 384 kbit/s and switches to 128 kbit/s after 50 seconds. The AQM parameter configuration is automatically changed when the RRC modifies the RB rate. Fig. 14 shows a trace for the SBD algorithm, using the parameter setting proposed in Table 3. When the bandwidth reduction takes place, the overbuffering is successfully avoided by means of reconfiguration.

Fig. 15 shows the same situation for an RED buffer. For each RB rate, RED is configured according to Table 5. The adaptive strategy is also effective for RED, although RED is less capable to avoid the overflow at the first stages of the connection, when the sources are in the *Slow Start* state. The increment of the buffer occupancy is

too steep for RED to react. SBD is specially designed to react against fast and sustained *BO* increments; therefore the overflow is avoided even in *Slow Start*.

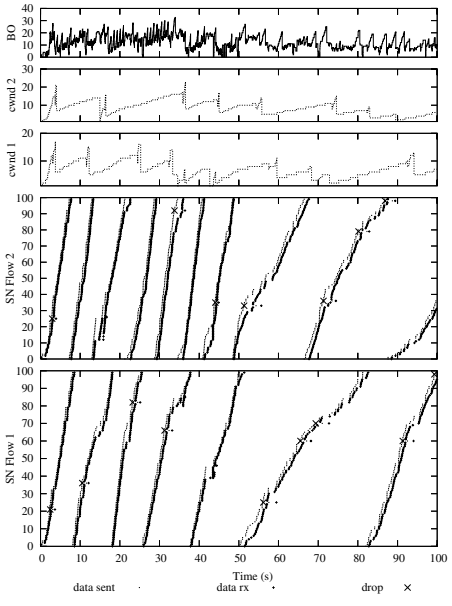


Fig. 14. Two TCP connections over RLC with automatic SBD reconfiguration

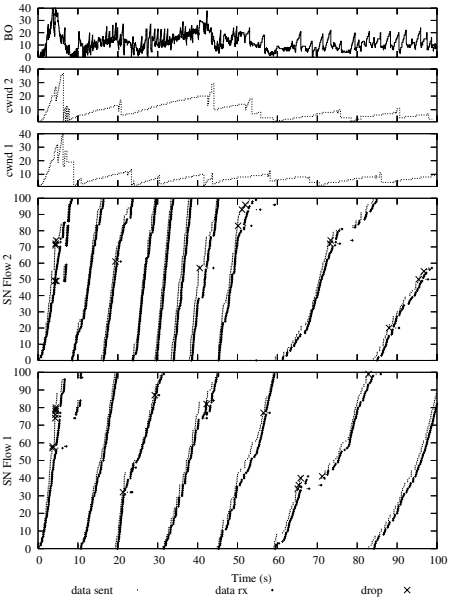


Fig. 15. Two TCP connections over RLC with automatic RED reconfiguration

7 Conclusions

This paper provides further insight into the effectiveness and configuration guidelines of AQM techniques on an RLC buffer. We focus on two AQM algorithms, RED and a novel deterministic scheme, SBD. By means of extensive simulation experiments we disclosed the effect of each parameter on TCP goodput and delay at different RB rates. Based on these results, we propose an optimum configuration for each algorithm aiming to reduce the delay while maintaining the goodput near the maximum. Compared to the current drop-tail specification of RLC, the delay performance is reduced about 45% and the goodput increases 12% for the single flow case.

SBD performs slightly better than RED in terms of delay reduction and its configuration is more straightforward. In addition, SBD is more effective than RED in avoiding buffer overflow in the first stages of the connection. This makes SBD a better choice than RED for applications requiring multiple downloads of short files, like Web surfing. Finally, SBD's deterministic operation makes it more feasible to implement on RLC, which operates in a per-user basis.

Finally, for each AQM scheme, we illustrate how a dynamic parameter reconfiguration is capable of maintaining an optimum performance, avoiding buffer overflow and excessive latency in situations of sudden changes in the RB bandwidth.

References

1. 3GPP TS 25.322, "Radio Link Control (RLC) protocol specification", v. 6.4.0., Jun. 2005.
2. M. Meyer, J. Sachs and M. Holzke, "Performance Evaluation of a TCP Proxy in WCDMA Networks", *IEEE Wireless Communication*, Oct. 2003, pp.70-79.
3. H. Inamura et al., "TCP over Second (2.5G) and Third (3G) Generation Wireless Networks" IETF RFC 3481, Feb. 2003.
4. R. Chakravorty, A. Clark and I. Pratt, "Optimizing Web Delivery over Wireless Links: Design, Implementation and Experiencies", *IEEE J. Select. Areas Commun.*, vol. 23, no. 2, Feb. 2005, pp. 402- 416.
5. M. Agfors, R. Ludwig, M. Meyer and J. Peisa, "Queue Management for TCP Traffic over 3G Links", in *Proc. IEEE WCNC 2003*, pp. 1663 -68.
6. J. J. Alcaraz, F. Cerdan and J. García-Haro, "Optimizing TCP and RLC Interaction in the UMTS Radio Access Network", *IEEE Network*, vol. 20, no. 2, Mar. 2006, pp. 56 – 64.
7. S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," *IEEE/ACM Trans. Networking*, vol. 1, pp. 397-413, Aug. 1993.
8. H. Holma, A. Toskala, *WCDMA for UMTS: Radio Access for Third Generation Mobile Communications, Third Edition*, Wiley, July 2004.
9. M. Rossi, L. Scaranari and M. Zorzi, "On the UMTS RLC Parameters Setting and their Impact on Higher Layers Performance", in *Proc. IEEE 57th VTC*, vol. 3, Oct. 2003, pp. 1827- 32.
10. R. Bestak, P. Godlewski and P. Martins, "RLC Buffer Occupancy when Using a TCP Connection over UMTS", in *Proc. IEEE PIMRC*, vol. 3. Sep. 2002, pp. 1161-65.
11. A. Gurtov, S. Floyd, "Modeling Wireless Links for Transport Protocols", *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, Apr. 2004, pp. 85-96.
12. A. Varga, "The OMNeT++ Discrete Event Simulation System", in *Proc. European Simulation Multiconference*. June 2001.
13. A. Chockalingam and M. Zorzi, "Wireless TCP Performance with Link Layer FEC/ARQ", in *Proc. IEEE ICC*, June1999, pp. 1212-16.

Performance Evaluation of Cross-Layer Routing for QoS Support in Mobile Ad Hoc Networks*

María Canales, José Ramón Gállego, Ángela Hernández-Solana, and Antonio Valdovinos

Institute of Engineering in Aragón, I3A, University of Zaragoza
C\ María de Luna, 3, 50.018, Zaragoza (Spain)
mcanales@unizar.es, jrgalleg@unizar.es, anhersol@unizar.es, toni@unizar.es

Abstract. Mobile ad hoc networks (MANETs) appear nowadays as one of the most promising architectures to flexibly provide multimedia services in multiple wireless scenarios. However, the dynamic nature of this environment complicates the supporting of the heavily demanded QoS. Since cooperation in MANETs is required to establish multihop communications, designing efficient QoS Routing algorithms mainly concentrates the technical efforts to guarantee QoS. This work presents a cross-layer architecture that performs a practical solution to solve the trade-off between the QoS provision and the efficient resource utilization thanks to different layers sharing network status information to cooperate in the network resource management. The cooperation between Routing and MAC levels allows to select End-to-End QoS paths according to the bandwidth availability measured in a realistic interference scenario, and appropriately react to mobility in a QoS context.

1 Introduction

Mobile ad hoc networks (MANETs) appear nowadays as one of the most promising architectures to flexibly provide multimedia services in multiple wireless scenarios. However, the dynamic nature of this environment makes it difficult to support the heavily demanded QoS. Cooperation in MANETs is required to establish multihop communications, relying on the nodes capability to act both as host and routers. The routing problem becomes more significant in this scenario, where resources are scarce and the routing protocol must be able to react to frequent topological changes and traffic variability without introducing excessive control overhead. In this situation, guaranteeing End-to-End QoS from the perspective of the network level is a difficult task.

In a wireless environment, the number of users that try to access is generally higher than the available radio resources. On the other hand an appropriate

* This work was financed by the Spanish Government (Project TEC2004-04529/TCM from MEC and FEDER), Gobierno de Aragón for WALQA Technology Park and the European IST Project PULSERS Phase II (IST - 027142).

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 322–333, 2006.

resource reservation according to the demands is required to obtain the desired QoS. Under these conditions, solving the trade-off between guaranteeing the requirements for the QoS provision with the highest efficiency in the use of the network resources is essential to maximize the system capacity. QoS support in MANETs involves the whole protocol stack of the network infrastructure [1]. One of the most promising ways to achieve the trade-off between the QoS provision and the efficient resource utilization is the cross-layer design (Fig. 1), which allows different layers to share network status information in order to cooperate in the network resource management.

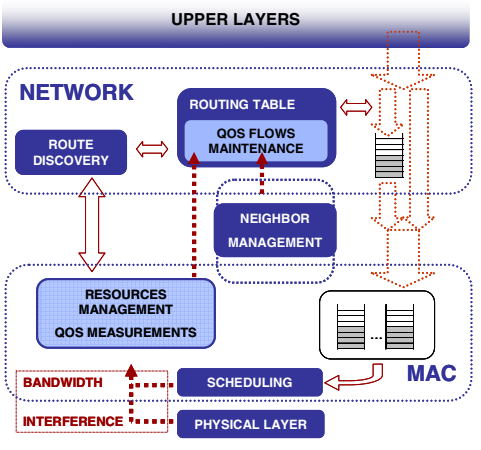


Fig. 1. Cross-layer Design for QoS Routing. General Architecture

The scope of most QoS Routing proposals only covers theoretical or heuristic approaches [2,3], without taking into account the potential problems of a practical implementation. Considering a realistic wireless ad hoc environment entails important physical implications that cannot be ignored to ensure the network capability to guarantee the demanded QoS. The interfering nature of the wireless medium and the lost of connectivity due to mobility affect any practical implementation, since collision-free transmissions cannot be assumed any more. This fact is especially critical on the control MAC level operations, such as connectivity maintenance or resource management. In order to validate any cross-layer proposal, it is necessary to consider the real implementation of the routing and MAC protocols to evaluate how they collaborate and the mechanisms that are actually considered to solve the QoS concept.

This work presents a QoS Routing based on a cross-layer operation that allows to identify the most appropriate path to cover the applications demands according to a new QoS metric. Thanks to the interaction between the routing and the MAC levels, this metric captures the resources availability, evaluating the capacity of providing QoS for an ongoing connection. The implemented architecture proposes the cooperation between a modified version of the Ad hoc

On-demand Multipath Distance Vector Routing (AOMDV) [4] and the ADHOC MAC protocol [5]. This solution has been evaluated in a scenario where Signal to Interference Ratio (SIR) and mobility considerations have been taken into account to overcome the problems stemmed from this dynamic environment.

The remaining of the paper is organized as follows. Section 2 presents the basis of the ADHOC MAC protocol, and the proposed QoS Routing protocol is described in Section 3, detailing the resource management mechanism. The solutions to the problems stemmed from the interference nature of the medium are introduced in Section 4 and the proposals to adapt the QoS routing operation to a mobility scenario are explained in Section 5. Simulations results are shown in Section 6. Finally, some conclusions are provided in Section 7.

2 The ADHOC MAC Protocol

Determining the bandwidth availability in an ad hoc environment is not an easy task and it is basically dependent on the current MAC layer. In this proposal, a MAC TDMA layer based on the ADHOC MAC protocol has been considered. ADHOC MAC works on a slot synchronous physical layer and implements a completely distributed access technique capable of dynamically establishing a reliable single-hop Basic broadcast CHannel (BCH) for each active terminal. Each BCH carries signaling information (FI – Frame Information), including priorities, which provides a prompt and reliable distribution of layer-two connectivity information to all the terminals.

When dealing with multimedia applications, in response to the demanded QoS, the MAC level must efficiently allocate resources for several differentiated services. To this purpose, the access and reservation strategies proposed in [6] have been considered in order to provide a reservation based mechanism to handle the access to data user resources and a simple but efficient traffic differentiation by exploiting the in band signaling provided by the ADHOC MAC protocol. The basis of this strategy relies on the use of the BCH capabilities to signal the request before the access, in such a way that collisions can be theoretically avoided (Book In Advance Strategy - BIAS). Preemption can be carried out in order to allocate resources for high priority services despite the lower priority ones. The policy used to resolve the conflicts in reservation is explained in detail in [6].

The ADHOC MAC protocol provides an efficient mechanism to measure the available bandwidth in terms of slots as well as ensures the reservation of the demanded ones. The core of the operation is the status information maintained by each terminal for all the slots in the TDMA frame. According to the information received in the BCH of each neighbor, related to the status they perceive (FREE, BUSY) a terminal defines its own slot status as RESERVED or AVAILABLE in order to select the resources to be allocated. This information is conditioned by the priority since higher priority services can steal resources to the lower ones. The complete rules to define this status are described in [6].

3 The QoS Routing Algorithm

A new QoS application is considered as a flow that needs a stable route during the whole connection. In the basic AODV (Ad hoc On-Demand Distance Vector [7] operation the source broadcasts requests packets *(RREQ)* referring this flow and each intermediate node rebroadcasts the first received copy of the RREQ until it reaches the destination, which sends a reply message *(RREP)* along the reverse path to the source. In terms of quality of service, several paths can satisfy the QoS requirements and the first request packet that reaches the destination does not actually identify the best path. The trade-off among different QoS requirements makes it difficult to choose the best solution. However, we can try to find a suboptimum path in terms of access delay but better satisfying the QoS requirements. The proposed QoS routing algorithm takes advantage of the multipath routing provided by the AOMDV to find several paths, although only one is selected according to a QoS metric based on the bandwidth requirements.

3.1 QoS Metric: Path Bandwidth Calculation Process

The AOMDV routing protocol has been adapted to include a modified version of the path bandwidth calculation algorithm described in [3] to measure the available bandwidth considering the whole path. The basic idea of this algorithm is to find the available TDMA slots that can be used for transmitting in every link along the path so that these slots, if reserved, would be interference-free. The measurement is performed and updated in each node during the discovery phase. The path bandwidth calculation ends in the destination node, and the calculated value represents the maximum available bandwidth between the source and the destination. The actual implementation of the algorithm operates as explained next.

According to the MAC level information, a node k is aware of the available slots for transmitting without interfering other connections (SRT_k set) and the available ones for receiving without collision (SRR_k set). Since in the ADHOC MAC protocol, preemption of reserved slots with lower priority is possible when resources of high priority are demanded, the set of available slots for the new QoS flow in the routing level will include these lower priority slots as available. During *RREQs* propagation, the set of available slots for communication in link *(i, j)* is calculated in node j and denoted as PB_{ij}. The set of transmitting slots must be disjoint in three consecutive hops to avoid collisions. According to this rule, each intermediate node appends its own SRT to the $RREQ$ packet, but also the PB_{ij} calculated in the previous two hops. With this information, in addition to the SRR, the next node receiving this $RREQ$ can calculate again the sets of slots to make them disjoint to the new link and update the appended information before forwarding the $RREQ$. The number of available slots in each set is reduced to the minimum value in the three hops used to compute them. When the destination node receives the $RREQ$, the dimension of the last availability set determines the total available bandwidth in the path. After waiting for several *RREQs* (multipath), one of the paths that match the requirements is selected according

to the metric. Then, the destination node sends the *RREP* packet through the reverse path to the source. The most updated information of the actual available set in every link is in the 3-hops-downstream neighbor. Therefore, to have an updated version of the available slots, during the reply phase a node appends to the *RREP* the more updated ones it has stored. When a node receives a *RREP*, it updates the sets to be forwarded, but also selects the effective slots to transmit, according to the demands, from the available set in the corresponding link. Then, the BIAS mechanism of the ADHOC MAC protocol is performed to effectively reserve these selected slots. The proposed solution acts as a distributed Call Admission Control (CAC) performed during the discovery process of the routing protocol [8]. An example of the whole process is shown in Fig. 2.

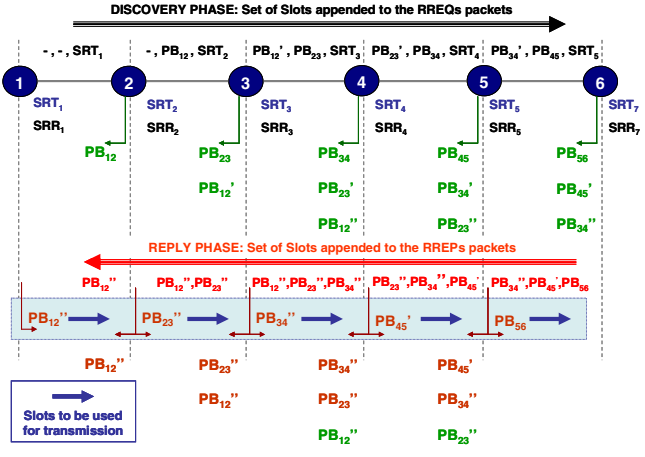


Fig. 2. Example of Path Bandwidth Calculation Process

The QoS metric computed along the path is given by (1)–(2):

$$BW_{metric}^{i,j} = |PB_{i,j}| \tag{1}$$

$$BW_{metric}^{PATH} = \min\left(BW_{metric}^{i,j}\right) \tag{2}$$

where $BW_{metric}^{i,j}$ is the measured BW value in the previous link (i, j), equal to the number of available slots (dimension of $PB_{i,j}$), and BW_{metric}^{PATH} is the more restrictive value in the whole path, equal to the last link BW_{metric}.

When an intermediate node receives a *RREQ* for a new flow, it updates the appended QoS metric in the *RREQ*, and evaluates if the QoS requirements are met. Only those packets received from paths with a valid metric are forwarded. A *RREQ* message is dropped if $BW_{metric}^{i,j} < N_{RREQ}$, the required slots. Repeated *RREQs* are not directly dropped in the destination node in order to perform a multipath operation so that several paths can be discovered and finally one can be selected, corresponding to the highest BW_{metric}^{PATH} and the lowest number of hops.

4 Operation in an Interference-Aware Scenario

In a typical scenario, connectivity among nodes is only based on Euclidean distances. In this situation, all nodes in the transmission range can correctly decode only one transmitted packet. If more than one neighbor transmits, a collision occurs. Transmissions one hop away are not sensed, which can lead to hidden-terminal [9] and exposed-terminal [10] problems, but if the MAC signaling can avoid them, as in the BIAS access scheme of the ADHOC MAC, totally collision-free transmissions are possible and the reuse capability is theoretically maximized.

However, in a more realistic scenario, where the actual interference produced by all the transmitting terminals is taken into account, collisions can still occur, leading to the loss of already reserved resources. The ability of decoding the received information is not only related to the distance of the transmitter and, in fact, the coverage range defined by one-hop neighbors varies according to the load conditions, as it is shown in Fig. 3. In this scenario, a transmission is considered successful if (3) is satisfied.

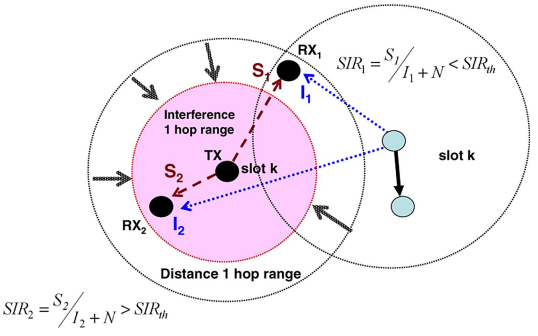


Fig. 3. Variations in the coverage range in a realistic interference scenario

$$SIR^k_{rx,i,j} = \frac{P^k_{tx,i} \cdot L_{i,j}}{P_{int} + P_{noise}} > SIR_{th} \tag{3}$$

$$P_{int} = \sum_{n \in N^k_{tx}, n \neq i} P^k_{tx,n} \cdot L_{n,j} \tag{4}$$

where $SIR^k_{rx,i,j}$ is the SIR received by terminal j from terminal i in slot k, $P^k_{tx,n}$ is the power transmitted by user n in slot k, $L_{n,j}$ is the path loss between users n and j, P_{int} is the total interference produced by other transmitting terminals, N^k_{tx} is the set of transmitting terminals in slot k, P_{noise} is the thermal noise and SIR_{th} is the minimum required SIR to be able to decode the information.

In order to provide more reliable link connections, the implemented MAC level includes a slot status, DIRTY, to identify slots where some power can be

sensed, although the terminal is not capable of decoding any information. A terminal cannot transmit in a slot that the potential receiver signals as DIRTY, assuming that the reservation may fail due to interference. Anyway, despite the DIRTY slot, collisions can still occur, even in a signaled as FREE slot. The interference power can be sensed if it exceeds a certain threshold, the Carrier Sense Threshold (CS_{th}). However, given a $P_{int} < CS_{th}$, which will lead to signal a slot as FREE, it can still happen that $SIR_{rx} < SIR_{th}$, especially when two terminals are neighbors but with a little margin for additional interference. In addition, even when the slot is correctly reserved, any new activation, although established between a distant pair of nodes, increases P_{int}, which can disrupt the ongoing transmission.

The negative effect of the not sensed interference or that created by new distant connections is even more critical over the BCH transmissions, since the carried control information is the basis for performing an appropriate resources allocation (BIAS access scheme) and for maintaining updated connectivity information. In fact, the cooperation with the network level can lead to wrong routing decisions due to this degraded MAC operation. The variability in the network activity as a consequence of these nodes trying to reallocate a BCH makes it more difficult to efficiently perform the resource management.

In this scenario, links between nodes that are actually in the coverage limit, have a very low margin to overcome this potential unexpected interference, therefore they are more likely to fail. In order to decrease this failure probability, then reducing the instability of the network, these links should be avoided.

As a first approximation, a partial solution can be performed in the network layer, via a new QoS metric to be included in the routing process, in addition to the measurement of the bandwidth demands. This metric evaluates the capability of the links to overcome additional interference providing and additional margin over the minimum required SIR to make the decoding correctly. The interlayer operation allows to use physical information to identify the quality of the link according to the received power and the measured SIR.

In [11] we show that this proposal allows to improve the global performance, specially the obtained throughput and delay for the admitted connections. However, this solution is applied for the QoS flows, although, as commented before, the more crucial effect is the instability generated in the network due to frequent BCH failures. Then, not only the QoS DATA packets need to be transmitted over reliable links, but also, and even more, the particular MAC BCH transmissions. In fact, the weakness of a link can be considered as a local characteristic that can be measured in the physical level. In order to provide this reliability to all connections (and also for best-effort traffic), an alternative to the SIR_{metric} is to transfer the same concept to the MAC level trying to provide a security margin to overcome the interference for any connection. An additional threshold $P_{rx,min}$ is used to verify the reliability of a link. This value is considered as the minimum received power to provide a theoretical SIR_{min} some dBs higher than SIR_{th} in the absence of any interference. Therefore, when a link is established under this condition, the effective $SIR^{k}_{rx,i,j}$ can be lower than the SIR_{min} due

to the interference but still higher than the SIR_{th}. In addition to (3), a reliable link must satisfy:

$$P^k_{rx,i,j} = P^k_{tx,i} \cdot L_{i,j} > P_{rx,min} \tag{5}$$

Weaker links, considered as those with a theoretical SIR_{rx} near SIR_{th}, are avoided since they will probably fail with slight increments of the interference in their environment, whereas those links covering both conditions can support higher levels of interference.

5 Mobility Management: QoS Monitoring

Once a path is selected, the variability in the network conditions would make unfeasible to maintain this path without a mechanism of QoS monitoring and path updating. In the normal operation of the AODV routing protocol nodes react to broken links sending error messages to inform the neighborhood about this event. New discoveries arise, as soon as the involved nodes realize the phenomenon, but this mechanism only alerts about broken links, assuming the path is unviable, whereas in a QoS environment links can be still viable although the bandwidth is not enough for covering the demands of a specific connection. Therefore, the routing algorithm must be capable of differentiating both effects making the terminals react appropriately according to the specific event.

The proposed updating process is performed using certain routing information piggy-backed in the *DATA–ACK* packets, similar to that sent during the *RREQ–RREP* phase, which allows to realize if the QoS constrains are not met anymore. Without calculating again a QoS metric, the sets of available slots are forwarded as in the discovery phase. These sets include the already reserved slots for this QoS flow. As a result, the process identifies the demanded bandwidth and the additional available one. Only when the interference has disrupted the reserved slots the piggy-backed *ACK* acts as a *RREP* packet that invokes in the MAC level the reservation of the new slots. Therefore, new resources, if available, can be reallocated without discovering a new path. If the QoS cannot be maintained after several updating phases (the number is configurable), a *QLOST (QoS LOST)* packet is sent to the source in order to trigger the discovery of a new path capable of satisfying the demanded bandwidth. When dealing with a QoS lost, the proposed scheme tries to find a new available path with the demanded QoS as during the discovery of a new path. However, despite the degradation of the QoS, the former path is sill viable to send traffic as best-effort. Therefore, this path is maintained to avoid dropping packets in excess while discovering an alternative QoS path. The changes in topology can make unfeasible to reallocate the connection with the demanded QoS. Then, maintaining the previous path as active avoids blocking the connection once it has been admitted. This blocking is considered more harmful than not admitting a new flow, since an established connection would suffer a non-tolerable degradation. Unless a new path covering the requirements is found releasing the previous one, the best-effort route keeps the connection active. When the updating process is triggered again, successive attempts to reallocate resources can finally lead to provide the demanded QoS.

When a broken link affects any path, a new discovery arises, as if it were a new connection to be admitted. However, if the affected path requires certain QoS, a new attempt to allocate resources may fail due to the new topology. Unlike the situation of the QoS lost, there is not a viable best-effort path to keep on sending packets. Then, if a new QoS path were not discovered, the connection would be blocked. To avoid this harmful degradation, the proposed QoS routing relaxes the constraints during the discovery of an already admitted but disrupted connection. The dropping policy applied by the intermediate nodes when receiving routing messages is not followed, in order to find the best available path, but including the best-effort alternative. The QoS metric is only used to classify the alternative paths. Anyway, if the connection is finally readmitted, the QoS updating process allows to subsequently reallocate resources if they are available. However, when the allocation of the disrupted connection is not possible, it is dropped to avoid colliding with the correctly dispatched ones.

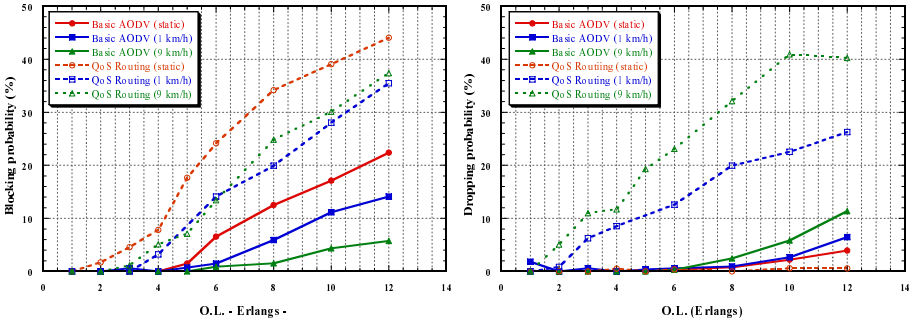
6 Performance Evaluation

In order to evaluate the performance of the proposal, we have built up a simulator in C++ which implements the functionalities of the design, considering the ADHOC MAC protocol interacting with the modified AOMDV, including the path-bandwidth calculation algorithm integrated in the routing process in a realistic ad-hoc environment. The connectivity among terminals is determined by the ability of decoding the BCH transmissions according to the received SIR, considering a transmitted power of 20 dBm, a Kammerman propagation model (6) and a minimum decoding threshold SIR_{th} of 5 dB. The SIR_{min} has been selected to 8.5 dB to overcome the problems of unexpected interference.

$$L_{i,j} = \begin{cases} 20 \cdot \log_{10}\left(\frac{4 \cdot \pi \cdot d}{\lambda}\right) & \text{if } d < 8, \\ 58.3 + 33 \cdot \log_{10}(\frac{\mathrm{d}}{8}) & \text{if } d \geq 8. \end{cases} \tag{6}$$

A set of 50 nodes are randomly positioned within a square area of 2 Km^2. Terminals follow the Random Waypoint (RWP) mobility model [12]. Several scenarios with average node speed of 1 and 9 km/h are simulated and compared to the performance in static conditions. Pause time in the RWP model is fixed to 2 seconds. Connections between different pairs of nodes are generated according to a Poisson process with rate [connections/sec.] ranging according to the simulated offered load and the mean connection duration (210 sec.). QoS flows are generated as CBR sources demanding a bandwidth of 64 kbps (2 TDMA slots). Packets exceeding a delay of 500 ms. are early discarded. In order to evaluate the proposed QoS routing, the measured parameters are delay of correctly received packets and throughput, calculated as the ratio among dispatched and offered traffic expressed in packets.

Figures 4 and 5 show the performance of the proposed architecture. The cross-layer operation acts as a distributed CAC that allows to efficiently allocate resources for the different connections leading to a better distribution of the resources occupation in the network.

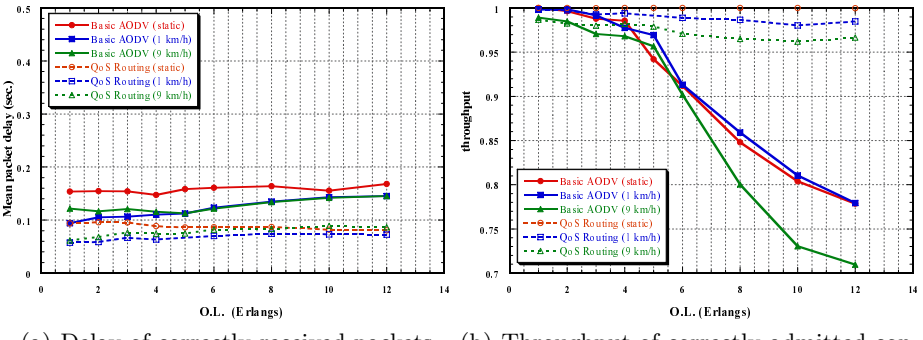


(a) Blocking probability (b) Dropping probability

Fig. 4. Performance of the proposed QoS Routing vs. the basic AODV operation. Failure probability: blocking of new connections and dropping of disrupted admitted connections.

When a new application cannot be allocated, the proposed routing does not find any available path not admitting the connection, which increases the number of blocked connections compared to the basic operation, as it is shown in figure 4(a). Even, when changes in the topology makes the network distribution unable to efficiently allocate the admitted connections, the disrupted ones are discarded, leading to a failure probability (figure 4(b)). However, this implies in fact a reduction on the congestion of the network which allows to better deal with the admitted connections, which experience lower delay, figure 5(a), and higher individual throughput, figure 5(b).

The individual improvement, in the end, leads to a higher global performance, as observed in figure 6, which shows that, even in a high mobility scenario, the QoS Routing outperformes the basic AODV operation in terms of correctly



(a) Delay of correctly received packets (b) Throughput of correctly admitted connections

Fig. 5. Performance of the proposed QoS Routing vs. the basic AODV operation. Evaluation of obtained the QoS for admitted connections (mean throughput and delay).

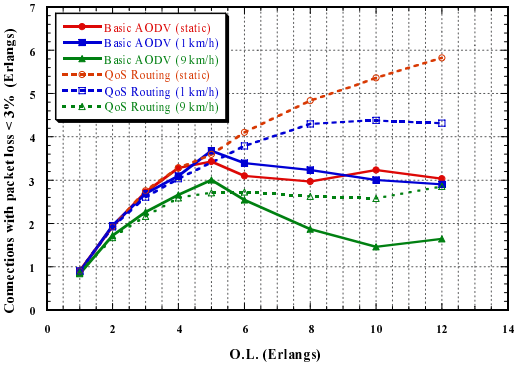


Fig. 6. Correctly dispatched connections with packet loss $< 3\%$

dispatched connections. A connection is considered correctly dispatched if it is not dropped and it achieves its expected QoS. The packet delay is limited thanks to the discarding policy, but the packet loss must be limited to the demanded restriction (considered 3 % in the simulations).

The better resource allocation is responsible of the packet discarding reduction, but its effectiveness in a mobility scenario is achieved thanks to the implemented QoS updating process. When a connection is admitted, the initial resource allocation allows to ensure certain bandwidth avoiding discarding packets due to congestion. However, in the dynamic environment, resources need to be reallocated due to the QoS lost. Thanks to the temporary maintenance of best-effort paths upon reception of a *QLOST* message, the packets dropping probability is reduced. While trying to rediscover a route with enough bandwidth, packets are still sent using these best-effort paths. Only when the allocation of new resources is not possible in the new topology, the connection is dropped in order to avoid disrupting the other ones. In the end, the response of the protocol to the interference variability (mobility / load increase) allows to maintain the desired QoS for the correctly dispatched connections.

7 Conclusions

This paper presents a QoS Routing based on a cross-layer architecture acting as a distributed admission control capable of efficiently allocating resources for bandwidth demanding applications. This proposal has been designed to overcome the problems stemmed from the interference nature of the wireless medium and the dynamic environment of mobile ad hoc networks.

The obtaining throughput gain of the proposed scheme is reduced as the nodes speed increases but in any case, this solution outperforms the basic AODV operation for any traffic load condition. The evaluation of the proposal in a realistic interference and mobility scenario has shown the capability of the cross-layer operation to react to the environment providing a soft-QoS even in a dynamic situation.

References

1. Mohapatra, P., Li, J., Gui, C.: QoS in mobile ad hoc networks. IEEE Wireless Communications (June 2003) 44–52
2. IEEE Journal on Selected Areas in Communications.: Special Issue on Wireless Ad Hoc Networks. Volume 17. (August 1999)
3. Zhu, C., Corson, M.: QoS routing for mobile ad hoc networks. In: Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'02). Volume 2., New York, USA (June 2002) 958–967
4. Marina, M., Das, S.: On-demand multi path distance vector routing in ad hoc networks. In: Proceedings of the International Conference on Network Protocols ICNP'01, Riverside, California, USA (2001) 14–23
5. Borgonovo, F., Capone, A., Cesana, M., Fratta, L.: ADHOC MAC: a new MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services. Wireless Networks (WINET) **10**(4) (July 2004) 359–366
6. Gállego, J.R., Canales, M., Hernández, A., Campelli, L., Cesana, M., Valdovinos, A.: Performance evaluation of point-to-point scheduling strategies for the AD-HOC MAC protocol. In: Proc. 8th International Symposium on Wireless Personal Multimedia Communications (WPMC'05), Aalborg (Denmark) (2005) 1380–1384
7. Perkins, C.E., Belding-Royer, E.M., Das, S.: Ad Hoc On-Demand Distance Vector (AODV) Routing. Experimental RFC 3561 (July 2003)
8. Canales, M., Gállego, J.R., Hernández, A., Valdovinos, A.: Cross-layer proposal for QoS routing in mobile ad-hoc networks. In: Proc. 8th International Symposium on Wireless Personal Multimedia Communications (WPMC'05), Aalborg (Denmark) (2005) 1325–1329
9. Tobagi, F.A., Kleinrock, L.: Packet switching in radio channels. part 2. The hidden terminal problem in carrier sense multiple-access and the busy-tone solution. IEEE Transactions on Communications **23**(12) (December 1975) 1417–1433
10. Haas, Z.J., Deng, J.: Dual Busy Tone Multiple Access (DBTMA): A multiple access control scheme for ad hoc networks. IEEE Transactions on Communications **50**(6) (June 2002) 975–985
11. Canales, M., Gállego, J.R., Hernández, A., Valdovinos, A.: Interference-aware routing with bandwidth requirements in mobile ad hoc networks. In: Proc. IEEE 62nd Semiannual Vehicular Technology Conference (VTC2005-fall), Dallas (USA) (2005)
12. Johnson, D.B., Maltz, D.A.: Chapter 5. In: Dynamic source routing in ad hoc wireless networks. Kluwer Academic Publishers (1996) 153–181

Medium Access Control with an Energy-Efficient Algorithm for Wireless Sensor Networks*

SangSoon Lim, SungHo Kim, JaeJoon Cho, and Sunshin An

Dept. of Electronics & computer Eng., Korea University,
1, 5-Ga, Anam-dong Sungbuk-ku, Seoul, Korea, Post Code: 136-701
{lssgood, shkim, jjj, sunshin}@dsys.korea.ac.kr

Abstract. This paper proposes an enhanced B-MAC (ENBMAC), a carrier sense Medium Access Control (MAC) protocol with ultra low power operations for wireless sensor networks. Due to battery-operated computing and sensing devices in wireless sensor networks, the development of MAC protocols that efficiently reduce power consumption is an important issue. B-MAC provides bidirectional interfaces such as Clear Channel Assessment (CCA), Low Power Listening (LPL) and uses an adaptive preamble sampling scheme to optimize performance and conserve energy. This reduces the amount of energy by comparing to other MAC protocols in WSNs. However, B-MAC can not achieve the overhearing avoidance. To solve this problem, we propose Node Recognition (NR) algorithm using the next hop address in MAC layer. Because this mechanism tries to handle the overhearing avoidance, ENBMAC makes it possible to extend the lifetime of the wireless sensor networks that contain a large number of nodes. The experiment results show that ENBMAC protocol reduces the energy consumed by receiving up to 90 percent comparing to B-MAC.

1 Introduction

Wireless sensor networks are generally composed of a large number of sensor nodes deployed to measure various physical information and a few data collectors, which are called sink nodes. Wireless sensor networks have recently become of significant interest due to cheap single-chip transceivers and micro controllers. They consist of many tiny devices, powered by small-sized batteries, and operate unattended for prolonged duration. Because sensor nodes may be deployed in remote locations, it is likely that replacing their battery will not be possible. Therefore, power efficient protocols at each layer of the communications are very important for wireless sensor networks [1]. In this paper, we will focus on the medium access control layer.

Conventional MAC protocols have been optimized for maximum throughput and minimum delay. Because of the target, they are not suitable for wireless sensor networks. To reach a major requirement of wireless sensor networks, several energy conserving MAC protocols have been proposed. For example, S-MAC employs the

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment).

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 334 – 343, 2006.

RTS/CTS/DATA/ACK signaling scheme, periodic listen and sleep to collision and overhearing avoidance, and message passing [2]. T-MAC is another example that dynamically adapts a listen and sleep duty cycle through fine-grained timeouts [3]. This protocol improves on S-MAC's energy usage by using an active period. The IEEE 802.15.4 uses periodic sleep to reduce energy consumption and requires synchronization to decide on suitable schedules [4]. B-MAC employs not only Clear Channel Assessment (CCA) and packet backoffs to avoid collisions, but also Low Power Listening (LPL) and preamble sampling to reduce duty cycle and minimize idle listening [5].

In this paper, we present ENBMAC protocol, which is an enhanced version of B-MAC. It tries to reduce the waste of energy consumed by overhearing. To achieve overhearing avoidance, ENBMAC employs Node Recognition (NR) algorithm without an additional overhead, while considering wireless sensor communication patterns and hardware limitations. The remainder of the paper is organized as follows. Section 2 summarizes reviews related work on MAC protocols and energy-saving solutions in WSNs. In section 3, we will elaborate on the design of the ENBMAC protocol. Then, in section 4, ENBMAC is evaluated through numerical analysis. Finally, section 5 concludes the paper.

2 Related Work

Because of various limitations and the characteristics of wireless sensor networks, the low power consumption is the main criterion for protocol design at every layer. The medium access control layer is one of the interesting research areas, and provides large opportunities of energy savings by dealing with the situations among nodes. There are several major sources of energy waste in wireless sensor networks: [2]

- ***Collision*** occurs when two nodes transmit at the same time and interfere with each others transmission. Hence, re-transmissions increase energy consumption.
- ***Control packet overhead*** such as RTS/CTS/ACK can be significant for wireless sensor networks that use small data packets.
- ***Overhearing*** means that there is no meaningful activity when nodes receive packets or a part of packets that are destined to other nodes.
- ***Idle listening*** is the cost of actively listening for potential packets. Because nodes must keep their radio in receive mode, this source causes inefficient use of energy.

To reduce energy consumptions by these factors, Polastre et al. develop a versatile low power MAC protocol called B-MAC, which is used as the default MAC for Mica2. By comparing B-MAC to conventional MAC protocol, e.g., IEEE 802.11 Distributed Coordinated Function (DCF), we know that B-MAC is more suitable for sensor networks, for it is optimized to conserve energy. In addition, B-MAC's flexibility results in better packet delivery rates, throughput, latency, and energy consumption than other MAC protocols in WSNs such as S-MAC, T-MAC. However, B-MAC suffers from the waste of energy consumed by overhearing. Since nodes do not know when they will be the receivers of messages from their neighbors, most energy in traditional MAC protocols is wasted by idle listening under low traffic loads. In addition, increasing the sample rate or neighborhood size increases the amount of traffic

in the network. As a result, each node consumes much energy by overhearing. There is an example related to overhearing problem in figure 1. Figure 1 shows the general communication architecture of WSNs [1]. When node A sends its physical information to the sink node, some neighboring nodes near node A overhear some packets that they do not need. These activities on the channel reduce energy efficiency of WSNs.

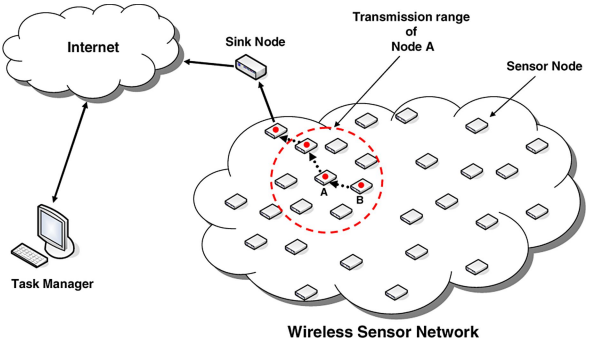


Fig. 1. The general architecture of Wireless Sensor Networks

3 Proposed ENBMAC Protocol Design

Energy dissipation includes three parts: energy dissipation on the sensor transducer, energy dissipation for communication among sensor nodes, and energy consumed by the microprocessor in computation. Since the part of communication consumes more power than other things, the mechanism, which reduces transmission and reception energy, is a necessary factor for MAC protocol design in WSNs. Although B-MAC employs an adaptive preamble sampling to reduce energy consumed by idle listening, it is not optimal. Overhearing from the neighbor nodes decreases energy efficiency.

ENBMAC provides a novel idea, called divided preamble sampling with overhearing avoidance scheme. While reducing the power consumption by the mechanism, ENBMAC preserves the basic properties of the original B-MAC protocol. The details of the implementation steps for ENBMAC protocol are described below sections.

3.1 ENBMAC Protocol

Figure 2 shows the transmission operation of the ENBMAC protocol. When a transmission of each node is requested from its application the node checks for a pending packet. If a pending packet is detected, transmission fails and the information related to the state of transmission is reported to upper layer that deals with retrying the operation. If the node can immediately transmit a packet, it saves the packet to the buffer and sets the random value of the initial backoff periods. After the operation, if the node is in sleep state, the algorithm of transmission puts the node into active mode to send the packet. In order to avoid collisions among neighboring nodes, the node delays for a random number of initial backoff periods and checks the status of the channel using CCA [5]. If there is no activity, the node constructs the MAC frame at once

and sends the packet to the destination node or the next hop node. Otherwise, the node performs additional backoffs until Retry Counter (RC) is equal to zero. After transmission, the node turns on the timer related to check interval and goes back to sleep mode. This mechanism is similar to a traditional carrier sense multiple access scheme; however, it returns to sleep mode to reduce energy consumption.

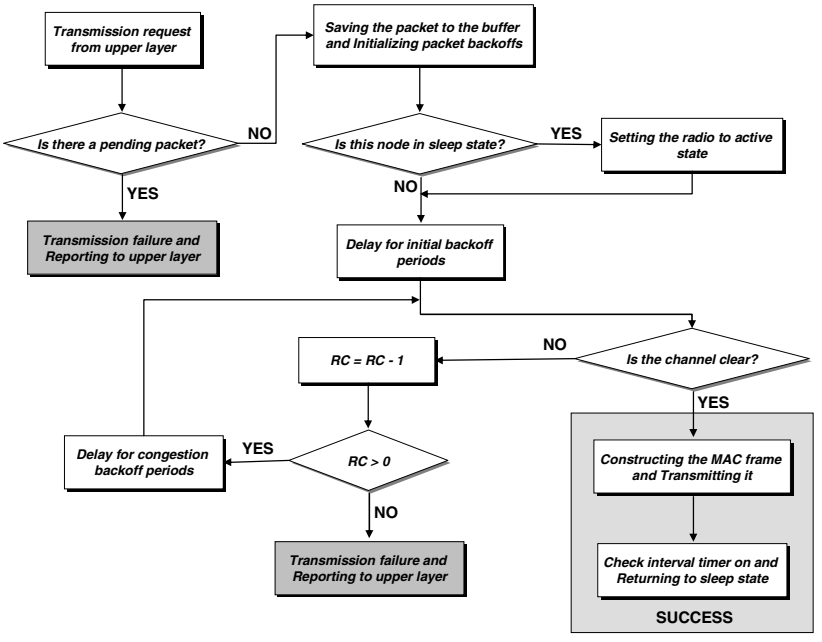


Fig. 2. ENBMAC Subroutine - Transmission

To achieve low power operation of reception, ENBMAC employs a variety of techniques such as divided preamble sampling, NR algorithm, CCA, and LPL (as shown in figure 3). Each node usually keeps up sleep state to minimize power consumption caused by idle listening and wakes up on a timer interrupt, named check interval timer. If the channel is active during check period, the node synchronizes with the preamble field of a preamble segment. A preamble segment consists of a part of preamble and the field of next hop address. After that, the node decodes a preamble segment and compares its address to the next hop address of the preamble segment. This scheme is called NR algorithm. If the incoming packet is destined to this node, the node receives the entire packet, turns on the check interval timer and returns to sleep state for avoiding idle listening. However, the node drops the remainder of the packet when its address is not matched to the next hop address through NR algorithm. From this algorithm, a lot of energy waste consumed by reception is reduced efficiently. To implement NR algorithm, the structure of long fixed preamble must be changed. The novel structure of preamble header and the NR algorithm are discussed more detail in section 3.2 and 3.3 respectively.

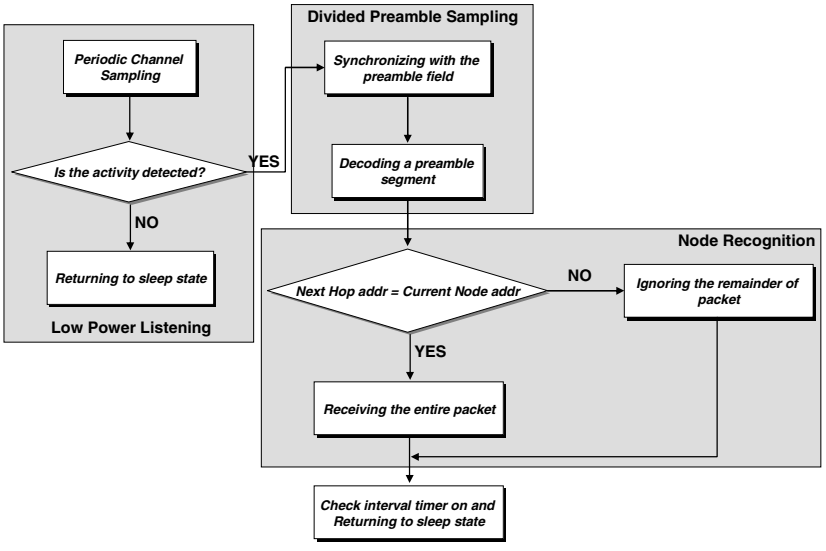


Fig. 3. ENBMAC Subroutine - Reception

3.2 Divided Preamble Sampling

All nodes that use B-MAC usually suffer from long and inefficient preambles. In order to overcome this drawback, a more effective structure and a sampling scheme are proposed. The structure of ENBMAC's entire preamble consists of several preamble segments as shown in figure 4.

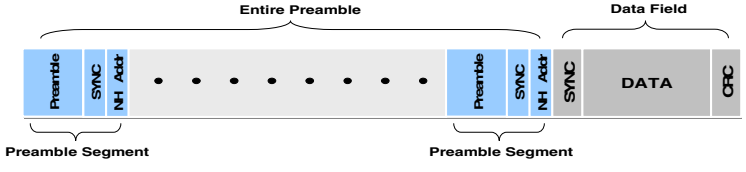


Fig. 4. The Structure of ENBMAC Frame

A preamble segment has three kinds of fields. The first is a preamble field that consists of the minimum length of bit pattern. The preamble length must be matched to the check interval when a node uses B-MAC protocol because of checking for activity on the channel reliably. If the channel is sampled every 100 ms, the entire preamble for detecting the activity must be at least 100 ms long. Although preamble is necessary for the bit synchronizer to synchronize correctly, a long and fixed preamble is not an essential factor to transmit packets. The minimum length of the preamble depends on the acquisition mode selected and the settling time. Typically, the preamble length is recommended by the manufacturer [6]. We employ the length in this field. The second is the SYNC field that notifies the end of short preamble for correct synchronization. The third field is the next hop address, which becomes a resource to

eliminate overhearing. When the node constructs a preamble segment, it obtains the information of next hop node from upper layer and adds the information to a segment. When a node has a packet requested from upper layer, it constructs the MAC frame with several preamble segments made up of the equal value to reliably receive packet. ENBMAC can provide the opportunity to ignore a large part of the entire packet through this structure.

3.3 Node Recognition Algorithm

B-MAC provides ultra low power operation, effective collision avoidance, and high channel utilization through a flexible interface. ENBMAC can operate a NR algorithm without destroying these advantages. It also has a flexible interface proposed in B-MAC and provides an additional interface related to the divided preamble sampling. As described in section 3.1, a node wakes up every check interval and detects activity on the channel, and receives the packet. At that time, the node that receives incoming packet does not need to listen to all parts of the packet if it is not a destination node or a next hop node. Figure 5 represents the basic example of transmission, reception, and overhearing avoidance of ENBMAC. If the packet transmitted by node A is destined to node C, node B can achieve low power reception with overhearing avoidance. There are no additional burdens in constructing MAC frame.

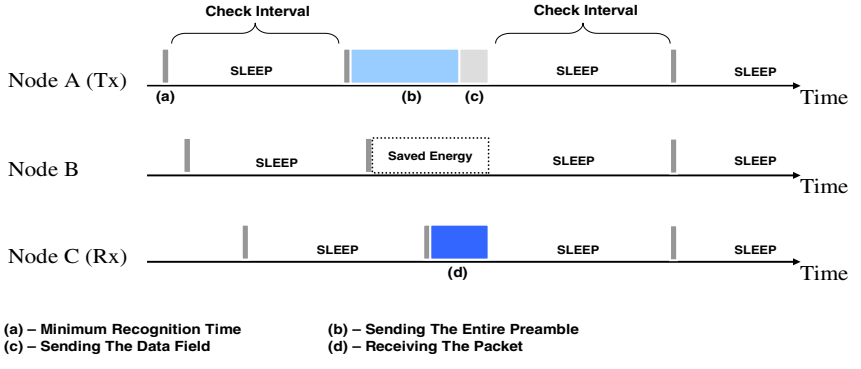


Fig. 5. The basic operations of ENBMAC protocol

At a starting point of a reception mode, a node must keep up the minimum recognition time in order to sense activity on the channel, fetch node address from a preamble segment, and compare node addresses. If a node cannot guarantee the recognition time, it is able to fail receiving the packet. To avoid this type of energy waste, ENBMAC must guarantee a period of turning on the radio and running NR algorithm. Therefore, the length of the entire preamble is defined as

$$L_{preamble} \times T_{txbyte} \geq T_{interval} + \alpha \tag{1}$$

where $L_{preamble}$ is the length of the entire preamble, T_{txbyte} and $T_{interval}$ are the time of sending one byte and the check interval time respectively, and α is the minimum

recognition time. After Manchester encoding in the CC1000 used in Mica2, the data rate is 19.2kbps [6]. Because we can get the value of T_{txbyte} from the data rate, $T_{interval}$ and α from the bidirectional interface, we are able to calculate the suitable length of the entire preamble.

4 Performance Evaluation

Basically, wireless sensor networks are able to support scalability of a network since the number of sensor nodes deployed in the field widely may be in the order of hundreds or thousands. In the case of B-MAC, the expansion of a network leads to the increase of total overhearing overhead. In order to offer the fault tolerance feature of WSNs, engineers have to provide high density networks. For this reason, more nodes that employ B-MAC suffer from serious overhearing problems, which result in a reduction of a network's lifetime. Therefore, if the traffic load or the number of nodes increases owing to various circumstances, B-MAC-applied-WSNs become exhausted from receiving no meaningful parts of packets. ENBMAC has accepted the properties of the existing B-MAC. Nevertheless, it is able to shorten energy exhaustion in many different ways.

In this section, the efficient factors of ENBMAC are shown through various equations and results. The focus is on comparing ENBMAC with B-MAC because B-MAC is shown to have higher throughput and better energy efficiency than S-MAC and T-MAC.

Table 1. Parameters for comparing ENBMAC and B-MAC

Parameter	Description	Values used in simulation
X_i	The waking up point of node i	Uniform Distribution
L_{packet}	Packet length of the application	40 Bytes
T_{txbyte}, T_{rxbyte}	Transmission and reception time of 1 byte	416us (19.2Kbps)
C_{rx}	Current used in reception mode	15 mA
C_{sleep}	Current used in sleep mode	0.03 mA
V	Voltage	3 V
$T_{arrival}$	Inter-arrival time of traffic	300 second (In a case of simple network)
$L_{preamble}$	In a case of simple network	151 Bytes (50ms), 271 Bytes (100ms), 391 Bytes (150 ms), 511 Bytes (200ms)
	In a case of multi-hop network	271 Bytes (fixed 100ms)
$N_c(i)$	The number of children nodes at node i	0~3 nodes

First, the simple one-hop network is considered. It is assumed that the network in figure 1 uses B-MAC and node B only transmits the sensing information to node A. The other nodes, except node B, regularly sense the surroundings and send information to the other nodes excluding node A. At that time, node A consumes much energy by overhearing caused by the six neighboring nodes except node B. Each of these six neighboring nodes has a different point of waking up time. Thus, in a case of a simple network, each node has an overhearing overhead as high as E_{over} per second.

$$E_{over} = \sum_{i=1}^{N-1} \left(\frac{(L_{preamble} + L_{packet} - X_i) \times T_{rxbyte} \times C_{rx} \times V}{T_{arrival}} \right) \quad (2)$$

In the case of ENBMAC, every node maintains a sleep state for overhearing duration after performing a NR algorithm. If the energy consumption of the additional sleep duration is E_{asleep}, we can calculate the quantity of E_{asleep} by replacing C_{rx} with C_{sleep} in equation (3). The saved energy by using ENBMAC is presented as:

$$E_{save} = E_{over} - E_{asleep} \quad (3)$$

Figure 6 represents the simulation result of the above equation using Table 1. We can understand how much overhearing is caused by check interval and the number of neighboring nodes through figure 6(a). If the node density or check interval increases, the number of bytes, which do overhear also rises. However, ENBMAC consumes in quantity of E_{asleep} instead of such overhearing energy as shown in figure 6(b).

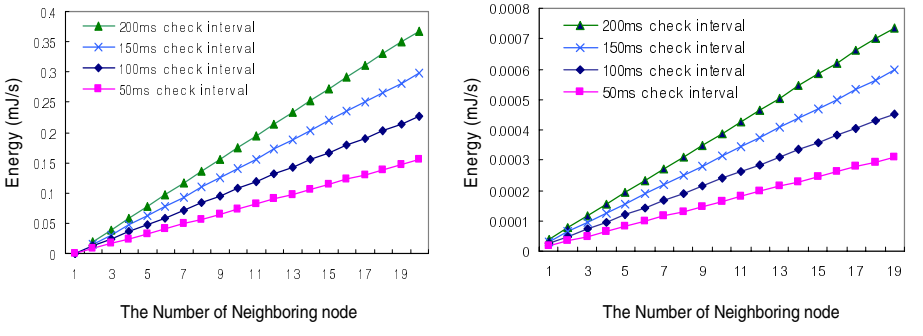


Fig. 6. The result of simple network

Finally, the effect of a multi-hop network is evaluated. In real wireless sensor networks, every node cannot be placed by one-hop distance from sink node. In this case, routing protocol is essential and the energy waste should come with a routing algorithm. The traffic through a node must include all the packets routed by the node and its neighbors. When there are N numbers of neighboring nodes in the viewpoint of one node, then transmit frequency per second is:

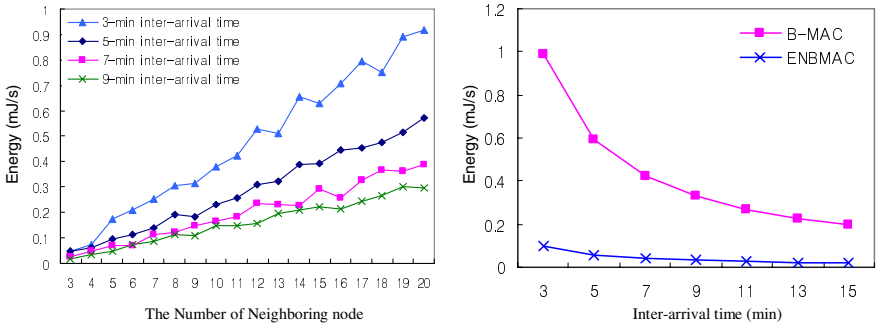
$$\frac{1}{T_{arrival}} \sum_{i=1}^{N} (N_c(i) + 1) \quad (4)$$

Therefore, while considering the real condition of WSNs, the quantity of saved energy of each node in ENBMAC is:

$$E_{save} = \sum_{i=1}^{N-N_c(0)} \left(\frac{(N_c(i) + 1)((L_{preamble} + L_{packet} - X_i) \times T_{rxbyte} \times C_{rx} \times V)}{T_{arrival}} \right) \quad (5)$$

where $N_c(0)$ is the number of children nodes itself.

Figure 7 shows the simulation result of a multi-hop network. According to figure 7(a), the shorter the inter-arrival time of traffic becomes, the more the traffic load increases and the greater amount of energy is saved by ENBMAC. In other words, ENBMAC is more suitable for the facts closely related to the transmit frequency such as inter-arrival time and node density. In figure 7(b), the comparison between ENBMAC and B-MAC shows that the former is able to save 90 percent of the reception energy per second in each inter-arrival time of the latter. By using the NR algorithm, ENBMAC eliminates the overhearing factor, the biggest weak point of B-MAC, and makes it possible to extend the lifetime of the wireless sensor networks.



(a) Overhearing energy **(b) Reception energy**

Fig. 7. The result of multi-hop network

The energy efficiency of ENBMAC is even better when nodes increase in number due to network expansion and node density in a specific area gets higher for fault tolerance. Furthermore, in the case of applying a routing condition, ENBMAC can work more on its own merits when transmission and reception get complicated and the number of communications becomes larger. Consequently, it is obvious that ENBMAC is far more efficient than B-MAC in supporting the properties of general WSNs efficiently. Overhearing can be reduced in the existing B-MAC when using the RTS-CTS mechanism. Nevertheless, it is not efficient to reserve channels using RTS-CTS mechanism in B-MAC. Because the reception node has to listen the channel status during a certain period to let the receiver hear RTS, the energy efficient operations of the node tend to be inefficient.

5 Conclusion

An energy-efficiency MAC protocol in Wireless Sensor Networks is an open research area in which we are conducting further studies. To solve the problem of overhearing and reach our goal in WSNs, we have proposed the ENBMAC protocol that employs NR algorithm. This protocol uses a novel idea, called divided preamble sampling to implement the mechanism. The structure of preamble segment provides various opportunities to improve energy efficiency. The performance results have shown the

ENBMAC protocol is more suitable for general WSNs and can achieve conserving energy in reception mode up to 90 percent comparing to B-MAC protocol.

This novel protocol is the subject of an ongoing study, and we plan to implement the ENBMAC protocol on the node that we made. Therefore, we expect more results related to energy efficiency, latency, and throughput in the future.

References

[1] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, A survey on sensor networks, IEEE Communications Magazine, Volume: 40. Issue: 8, pp. 102-114, August 2002.

[2] W. Ye, J. Heidemann, and D. Estrin. An energy-efficient mac protocol for wireless sensor networks. In In Proceedings of the 21st International Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002), New York, NY, June 2002.

[3] T. van Dam and K. Langendoen. An adaptive energy-effcient MAC protocol for wireless sensor networks. In Proceedings of the First ACM Conference on Embedded Networked Sensor Systems (SenSys), Los Angeles, CA, November 2003.

[4] IEEE, Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANS), IEEE 802.15.4-2003, 2003.

[5] J. Polastre, J. Hill, and D. Culler. Versatile low power media access for wireless sensor networks. In Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys), Baltimore,MD, November 2004.

[6] Chipcon Coporation. Single Chip Very Low Power RF Transceiver. http://www.chipcon.com/files/CC1000_Data_Sheet_2_1.pdf, Apr. 2002

[7] El-Hoiyi, J.-D. Decotignie, and J. Hernandez. Low power MAC protocols for infrastructure wireless sensor networks. In Proceedings of the Fifth European Wireless Conference, Feb. 2004.

[8] El-Hoiydi, Aloha with Preamble Sampling for Sporadic Traffic in Ad Hoc Wireless Sensor Networks, in Proc. IEEE Int. Conf. on Communications, New York, USA, Apr 2002, pp. 3418–3423.

[9] University of California, Berkeley. TinyOS CVS Repository at SourceForge. http://sf.net/projects/tinyos/, 2005.

Giving Neurons to Sensors: An Approach to QoS Management Through Artificial Intelligence in Wireless Networks

Julio Barbancho, Carlos León, Javier Molina, and Antonio Barbancho

Department of Electronic Technology, University of Seville.
C/ Virgen de Africa, 7. Seville 41011, Spain
Tel.: (+034) 954 55 71 92; Fax: (+034) 954 55 28 33
{jbarbancho, cleon, fjmolina, ayboc}@us.es

Abstract. For the latest ten years, many authors have focused their investigations in wireless sensor networks. Different researching issues have been extensively developed: power consumption, MAC protocols, self-organizing network algorithms, data-aggregation schemes, routing protocols, QoS management, etc. Due to the constraints on data processing and power consumption, the use of artificial intelligence has been historically discarded. However, in some special scenarios the features of neural networks are appropriate to develop complex tasks such as path discovery. In this paper, we explore the performance of two very well known routing paradigms, *directed diffusion* and *Energy-Aware Routing*, and our routing algorithm, named **SIR**, which has the novelty of being based on the introduction of neural networks in every sensor node. Extensive simulations over our wireless sensor network simulator, OLIMPO, have been carried out to study the efficiency of the introduction of neural networks. A comparison of the results obtained with every routing protocol is analyzed. This paper attempts to encourage the use of artificial intelligence techniques in wireless sensor nodes.

Keywords: Wireless sensor networks (WSN); Ad hoc networks, Quality of service (QoS); Artificial neural networks (ANN); Routing; Self-Organizing Map (SOM), ubiquitous computing.

1 Introduction

In recent years technological advances have made the manufacturing of small and low-cost sensors economically and technically possible. These sensors can be used to measure ambient conditions in the environment surrounding them. Typically, wireless sensor networks (WSNs) contain hundreds or thousands of those sensors nodes. Due to the sensor features (low-power consumption, low radio range, low memory, low processing capacity, and low cost), self-organizing network is the best suitable network architecture to support applications in such a scenario. Goals like efficient energy management [1], high reliability and availability, communication security, and robustness have become very important

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 344–355, 2006.

issues to be considered. This is one of the many reasons why we can not neglect the study of the collision effects and the noise influence.

Many research centers worldwide (specially in Europe and USA) have focused their investigations on this kind of networks. Ian Akyldiz et al. [2] and Holger Karl et al. [3] have made great effort to describe the state-of-the-art of this subject.

Our research group, Computer Science for Industrial Applications, from the University of Seville, is working on the development of protocols and system architectures on Wireless Sensor Networks to support Supervisory Control and Data Acquisition (SCADA) applications. We present in this paper a new routing algorithm which introduces artificial intelligence (AI) techniques to measure the QoS supported by the network.

This paper is organized as follows. In section 2, we relate the main routing features we should consider in a network communication system. A description of the defined network topology is given. Section 3 introduces the use of neural networks in sensors for determining the quality of neighborhood links, giving a QoS model for routing protocols. The performance of the use of this technique in existing routing protocols for sensor networks is evaluated by simulation in section 4. Concluding remarks and future works are given on section 5.

2 Designing the Network Topology

The WSN architecture as a whole has to take into account different aspects, such as the protocol architecture; Quality-of-Service, dependability, redundancy and imprecision in sensor readings; addressing structures, scalability and energy requirements; geographic and data-centric addressing structures; aggregating data techniques; integration of WSNs into larger networks, bridging different communication protocols; etc.

Due to the desire to cover a large area, a communication strategy is needed. there are many studies that approach the problem of high connectivity in wireless ad hoc networks [4], [5]. In our research we consider a random distribution of sensors.

In general, routing in WSNs can be divided into *flat-based* routing, *hierarchical-base* routing, and *location-based* routing. In this paper we study networks where all nodes are supposed to be assigned equal roles or functionalities. In this sense, flat-based routing is best suited for this kind of networks.

Among all the existing flat routing protocols, we have chosen *directed diffusion* and *Energy-Aware Routing* (*EAR*) to evaluate the influence of the use of AI techniques.

In directed diffusion [6], sensors measure events and create gradients of information in their respective neighborhoods. The base station request data by broadcasting interests. Each sensor that receives the interest sets up a gradient toward the sensor nodes from which it has received the interest. This process continues until gradients are set up from the sources back to the base station.

EAR [7] is similar to directed diffusion. Nevertheless it differs in the sense that it maintains a set of paths instead of maintaining or enforcing one optimal

path at higher rates. These paths are maintained and chosen by means of a certain probability. The value of this probability depends on how low the energy consumption that each path can achieve is. By having paths chosen at different times, the energy of any single path will not deplete quickly.

3 Introducing Neurons in Sensor Nodes

The necessity of connectivity among nodes introduces the routing problem. In a WSN we need a multi-hop scheme to travel from a source to a destiny. The paths the packets have to follow can be established based on a specific criterion. Possible criteria can be minimum number of hops, minimum latency, maximum data rate, minimum error rate, etc. For example, imagine that all the nodes desire to have a path to route data to the *base station*[1]. In this situation, the problem is solved by a technique called *network backbone formation*.

Our approach to enhance this solution is based on the introduction of artificial intelligence techniques in the WSNs: expert systems, artificial neural networks, fuzzy logic and genetic algorithms. Due to the processing constraints we have to consider in a sensor node, the best suited, among all these techniques, is the *self-organizing-map* (*SOM*). This is kind of artificial neural network based on the self organization concept.

SOM is an unsupervised neural network. The neurons are organized in an unidirectional two layers architecture. The first one is the input or sensorial layer, formed by m neurons, one per each input variable. These neurons work as buffers distributing the information sensed in the input space. The input is formed by stochastic samples $\boldsymbol{x}(t) \in \boldsymbol{\mathcal{R}}^m$ from the sensorial space. The second layer is usually formed by a rectangular grid with $nx\mathrm{x}n'y$ neurons. Each neuron (i, j) is represented by an m-dimensional weight or reference vector called *synapsis*, $\boldsymbol{w'}_{ij} = [w'_{ij1}, w'_{ij2}, \ldots, w'_{ijm}]$, where m is the dimension of the input vector $\boldsymbol{x}(t)$. The neurons in the output layer -also known as the competitive Kohonen layer- are fully connected to the neurons in the input layer, meaning that every neuron in the input layer is linked to every neuron in the Kohonen layer. In SOM we can distinguish two phases: the ***learning phase***, in which, neurons from the second layer compete for the privilege of learning among each other, while the correct answer(s) is (are) not known; and the ***execution phase***, in which every neuron (i, j) calculates the similarity between the input vector $\boldsymbol{x}(t)$, $\{x_k \mid 1 \leq k \leq m\}$ and its own synaptic-weight-vector $\boldsymbol{w'}_{ij}$.

3.1 Network Backbone Formation

This problem has been studied in mathematics as a particular discipline called *Graph Theory*, which studies the properties of graphs.

A *directed graph* G is an ordered pair $G := (V, A)$ with V, a set of vertices or nodes, v_i, and A, a set of ordered pairs of vertices, called *directed edges*, *arcs*, or *arrows*.

[1] In WSN, we often consider two kind of nodes, base stations and sensor nodes. There is usually only one base station.

An edge $v_{xy} = (x, y)$ is considered to be directed from x to y; where y is called the head and x is called the tail of the edge.

In 1959, E. Dijkstra proposed an algorithm that solves the single-source shortest path problem for a directed graph with nonnegative edge weights.

We propose a modification on Dijkstra's algorithm to form the network backbone, with the minimum cost paths from the base station or *root*, r, to every node in the network. We have named this algorithm Sensor Intelligence Routing, **SIR** [8].

3.2 Quality of Service in Wireless Sensor Networks

Once the backbone formation algorithm is designed, a way of measuring the edge weight parameter, w_{ij}, must be defined. On a first approach we can assume that w_{ij} can be modelled with the number of hops. According to this assumption, $w_{ij} = 1 \ \forall \ i, j \in \mathcal{R}, i \neq j$. However, imagine that we have another scenario in which the node v_j is located in a noisy environment. The collisions over v_j can introduce link failures increasing power consumption and decreasing reliability in this area. In this case, the optimal path from node v_k to the root node can be p', instead of p. It is necessary to modify w_{ij} to solve this problem. The evaluation of the QoS in a specific area can be used to modify this parameter.

The traditional view of QoS in communication networks is concerned with end-to-end delay, packet loss, delay variation and throughput. Numerous authors have proposed architectures and integrated frameworks to achieve guaranteed levels of network performance [9]. However, other performance-related features, such as network reliability, availability, communication security and robustness are often neglected in QoS research. The definition of QoS requires some extensions if we want to use it as a criterion to support the goal of controlling the network. This way, sensors participate equally in the network, conserving energy and maintaining the required application performance.

We use a QoS definition based on three types of QoS parameters: timeliness, precision and accuracy. Due to the distributed feature of sensor networks, our approach measures the QoS level in a spread way, instead of an end-to-end paradigm. Each node tests every neighbor link quality with the transmissions of a specific packet named *ping*. With these transmissions every node obtains mean values of latency, error rate, duty cycle and throughput. These are the four metrics we have defined to measure the related QoS parameters.

Once a node has tested a neighbor link QoS, it calculates the distance to the root using the obtained QoS value. The expression 1 represents the way a node v_i calculates the distance to the root through node v_j, where *qos* is a variable whose value is obtained as an output of a neural network.

$$d(v_i) = d(v_j) \cdot qos \tag{1}$$

4 Performance Evaluation by Simulation

Due to the desire to evaluate the SIR performance, we have created two simulation experiments running on our wireless sensor network simulator OLIMPO

[10]. Every node in OLIMPO implements a neural network (SOM) running the execution phase (online processing).

4.1 Radio Channel Analytical Performance Evaluation

In order to accurately model the sensor networks, the wireless channel is equipped with certain propagation models which allows sensors to determine the strength of the incoming signal. These models are integrated in the channel object of the simulation tool.

For the purpose of this research, the values shown in table 1 have been considered.

Table 1. Values of radio communication parameters

Resonating frequency†:	869.85 MHz	Communication bandwidth† B:	0.5 %
Number of radio channels†:	1	Antenna gain‡:	$G_r = 1$, $G_t = 1$
Radio transmitter power:	$P_t = 5mW$	Radio receiver sensibility:	$P_s = -101dB$
System loss	$L = 1$	Path loss exponent:	$n = 2$
Modulation:	FSK	Transmission rate, R:	4800 b/s
Input noise power density N_{in}:	-174 dBm/Hz	Noise Figure $(NF)_{dB}$:	10 dB

†Based on licensed free standard ETSI EN 301 291.

‡Antennas are assumed to be omnidirectional.

In this scenario, two sensor nodes attempting to establish a radio communication link can be 218 meters separated[2]. In our simulations we have assumed that the distance between every pair of sensor nodes is set up randomly. We have focused our simulation on a wireless sensor network composed by 250 nodes.

4.2 Noise Influence

Noise influence over a node has been modelled as an Additive Gaussian White Noise, (AWGN), originating at the source resistance feeding the receiver. According to the radio communication parameters detailed in table 1 we can determine the signal-to-noise ratio at the detector input with the equation 2 [11], $S/N_d = 26.7\ dB$. This signal-to-noise ratio can be expressed as an associated BER (Bit Error Rate)[3]. If S/N_d is less than $26.7\ dB$ the receiver can't detect any data on air. An increase of the noise can degrade the BER. In another way, due to the relation between E_b/N_o and the transmission rate (R), $E_b/N_o = (S/R)/N_o$, an increase of R can also degrade the BER.

$$(P_s)_{dBm} = (N_{in})_{dB} + (NF)_{dB} + (10 \log B)_{dB} + (S/N)_d \tag{2}$$

To evaluate the effect of noise we have defined a node state declared as *failure*. When the BER goes down below a required value (typically 10^{-3}) we assume

[2] According to free space propagation model [11].

[3] The minimum probability of bit error $P_{e,min}$, in a FSK system with an adaptative filter at the radio receiver, is typically expressed in the literature with the expression: $P_{e,min} = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_o}}\right)$, where $\frac{E_b}{N_o} = \frac{(S/R)}{N_o} = \frac{S}{N}$.

this node has gone to a failure state. We measure this metric as a percentage of the total lifetime of a node. In section 4 we describe two experiments according to different percentages of node failures.

4.3 SOM Creation

Our SOM has a first layer formed by four input neurons, corresponding with every metric defined in section 3.2 (latency, throughput, error rate and duty cycle); and a second layer formed by twelve output neurons forming a 3x4 matrix.

Next, we detail our SOM implementation process.

Learning phase: In order to organize the neurons in a two dimensional map, we need a set of input samples $\boldsymbol{x}(t)$=[latency(t), throughput(t), error-rate(t), duty-cycle(t)]. This samples should consider all the QoS environments in which a communication link between a pair of sensor nodes can work. In this sense, we have to simulate special ubiquitous computing environments. These scenarios can be implemented by different noise and data traffic simulations. In our research we create several WSNs over OLIMPO with 250 nodes and different levels of data traffic. The procedure to measure every QoS link between two neighbors is detailed as follows: every pair of nodes (eg. v_i and v_j) is exposed to a level of noise. This noise is introduced increasing the noise power density N_o in the radio channel in the proximity of a determined node. Hence, the signal-to-noise ratio at the detector input of this selected node decreases and consequently the BER related with its links with every neighbor gets worse.

In order to measure the QoS metrics related with every N_o, we run a ping application between a selected pair of nodes (eg. v_i and v_j). Node v_i sends periodically a ping message to node v_j. Because the ping requires acknowledgment (ACK), the way node v_i receives this ACK determines a specific QoS environment, expressed on the four metrics elected: latency (seconds), throughput (bits/sec), error rate (%) and duty cycle(%). For example, for a noise power density of $N_o = -80\ dBm/Hz$ and a distance of separation[4] between node v_i and node v_j of 60 meters the QoS measured in node v_i and expressed in the metrics defined is [0.58, 1440, 10.95, 2.50]. This process is repeated 100 times with different N_o and d. This way, we obtain a set of samples which characterize every QoS scenario.

With this information, we construct a self-organizing map using a high performance neural network tool, such as MATLAB®, on a Personal Computer. This process is called *training*, and uses the learning algorithm. Because the training is not implemented by the wireless sensor network, we have called this process *offline processing*.

[4] Considering the free space propagation model, the power transmitted from the source decreases according the expression $P_r = P_t \left[\frac{\lambda}{4\pi dL}\right]^2 G_t G_r$, where P_r, is the radio power received at a distance d from the transmitter; P_t is the transmitter signal power, G_t and G_r are the antenna gains of the transmitter and the receiver respectively; L ($L \leq 1$) is the *system loss* and λ is the electromagnetic wavelength.

Once we have ordered the neurons on the Kohonen layer, we identify each one of the set of 100 input samples with an output layer neuron. According to this procedure, the set of 100 input samples is distributed over the SOM.

The following phase is considered as the most difficult one. The samples allocated in the SOM form groups, in such a way that all the samples in a group have similar characteristics (latency, throughput, error rate and duty cycle). This way, we obtain a map formed by clusters, where every cluster corresponds with a specific QoS and is assigned a neuron of the output layer. Furthermore, a synaptic-weight matrix $\boldsymbol{w'}_{ij} = [w'_{ij1}, w'_{ij2}, \ldots, w'_{ij4}]$ is formed, where every synapsis identifies a connection between input and output layer.

In order to quantify the QoS level, we study the features of every cluster and, according to the QoS obtained in the samples allocated in the cluster, we assign a value between 0 and 10. As a consequence, e define an output function $\Theta(i,j), i \in [1,3], j \in [1,4]$ with twelve values corresponding with every neuron $(i,j), i \in [1,3], j \in [1,4]$. The highest assignment (10) must correspond to that scenario in which the link measured has the worst QoS predicted. On the other hand, the lowest assignment (0) corresponds to that scenario in which the link measured has the best QoS predicted. The assignment is supervised by an engineer during the offline processing.

Execution phase: As a consequence of the learning phase, we have declared an output function, that has to be run in every sensor node. This procedure is named the *wining neuron election algorithm.*

In the execution phase, we create a WSN with 250 nodes. Every sensor node measures the QoS periodically running a ping application with every neighbor, which determines an input sample. After a node has collected a set of input samples, it runs the wining neuron election algorithm. For example, if a specific input sample is quite similar than the synaptic-weight-vector of neuron (2,2), this neuron will be activated. After the winning neuron is elected, the node uses the output function Θ to assign a QoS estimation, *qos*. Finally, this value is employed to modify the distance to the root (eq. 1). Because the execution phase is implemented by the wireless sensor network, we have called this process *online processing.*

4.4 Evaluating SIR Performance

Our SIR algorithm has been evaluated by the realization of three experiments detailed as follows.

Experiment #1: No node failure. The purpose of this experiment is to evaluate the introduction of AI techniques in a scenario were there is no node failure. This means that no node has gone to a failure state because of noise, collision or battery fail influence.

To simulate this scenario, a wireless sensor network with 250 nodes is created on our simulator OLIMPO. Node # 0 is declare as a sink and node # 22 is declared as a source. At a specific time, an event (eg. an alarm) is

provoked in the source. Consequently, the problem now is how to route the event from the specified source to the declared sink.

As detailed in section 2 we solve this problem with three different routing paradigms: SIR, directed diffusion and EAR. We choose two metrics to analyze the performance of SIR and to compare it to others schemes. These metrics are:

- Average dissipated energy. This metric computes the average work done by a node a in delivering useful tracking information to the sinks. This metric also indicates the overall lifetime of sensor nodes.

  According to the first energy consumption order model proposed by Wendi Rabiner Heinzelman in the *LEACH* protocol [12], we can assume the radio dissipates $E_{elec} = 50\ nJ/bit$ to run the transmitter or receiver or receiver circuitry, and $\varepsilon_{amp} = 100\ pJ/bit/m^2$ for the transmit amplifier to achieve an acceptable $\frac{E_b}{N_o}$ (figure 1). This way, to transmit a k-bit

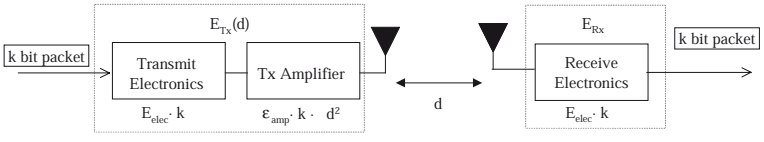


Fig. 1. Energy model

message a distance d using this radio model[5], the radio expends:

$$E_{Tx}(k, d) = E_{elec} \cdot k + \varepsilon_{amp} \cdot k \cdot d^2 \tag{3}$$

and to receive this message, the radio expends:

$$E_{Rx}(k) = E_{elec} \cdot k \tag{4}$$

We assume that the radio channel is symmetric, and that our simulation is *event-driven*, that is, sensors only transmit data if some event occurs in the environment. Due to transmission distance from a sensor node to the base station is large on a global scale, the transmission energy is much more higher than the received energy. In this network topology, as detailed in section 2, the most energy-efficient protocol is the minimum-transmission-energy.

- Average Delay. This metric measures the average one-way latency observed between transmitting an event and receiving it at each sink.

We study these metrics as a function of sensor network size. The results are shown in figure 2.

Experiment #2: 20 % simultaneous node failures. The purpose of this experiment is to evaluate the introduction of AI techniques in a scenario where there is a 20 % of simultaneous node failures. This means that at any

[5] We assume the radio propagation model.

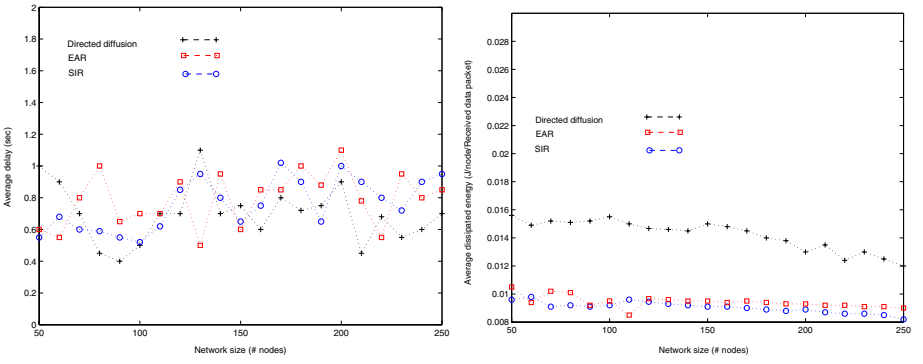


Fig. 2. Average latency and average dissipated energy in a scenario with no simultaneous node failure

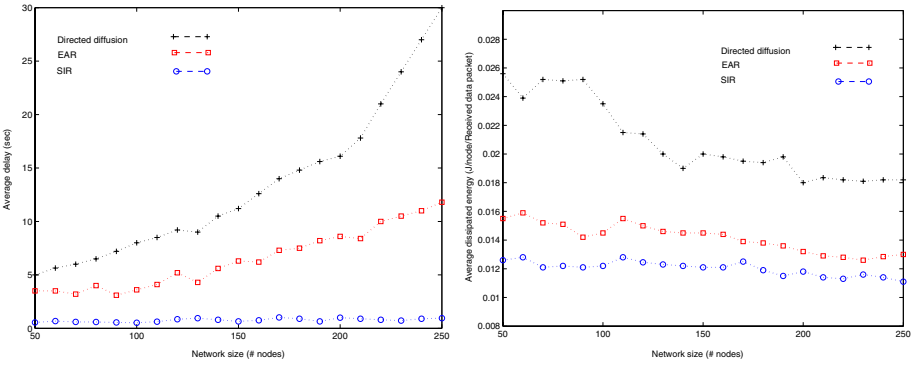


Fig. 3. Average latency and average dissipated energy in a scenario with 20 % simultaneous node failures

instant, 20 % of the nodes in the network are unusable because of noise, collision or battery failure influence.

To simulate these situations we create a WSN with 250 nodes. Amongst all of them, we select 20 % of the nodes (50) to introduce one of the following effects:

- S/N ratio degradation. Due to battery energy loss, the radio transmitter power decays. Consequently, the S/N ratio in its neighbors radio receivers is degraded, causing no detections with a certain probability, P. In this situation, we can assume that the node affected by the lack of energy is prone to failure with probability P.
- In many actual occasions, sensor nodes are exposed to high level of noise, caused by inductive motors. Furthermore, the radio frequency band[6] is shared with other applications that can interfere with our WSN.

[6] The use of this band is regulated in Europe by the European Conference of Postal and Telecommunications Administrations (CEPT) and the European Telecommunications Standards Institute (ETSI) by the technical standard *EN 300 220-1*.

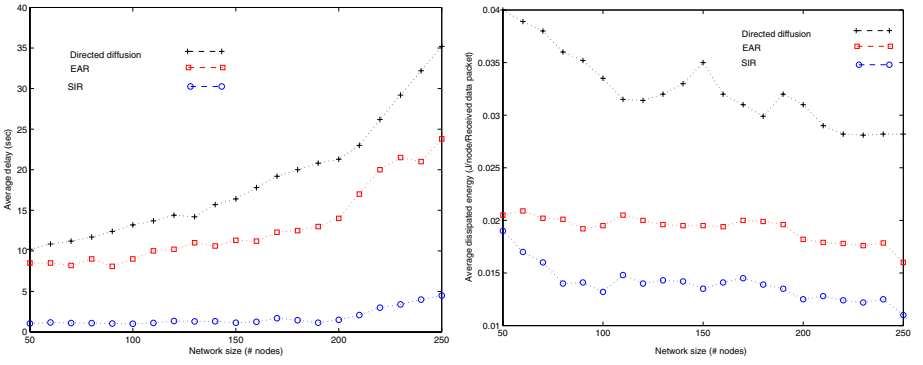


Fig. 4. Average latency and average dissipated energy in a scenario with 40 % simultaneous node failures

In these scenario we analyze the problem studied described in experiment #1 with the three paradigms related. The results are shown in figure 4.

Experiment #3: 40 % simultaneous node failures. This experiment simulates a scenario with a 40 % of simultaneous node failures.

5 Conclusion and Future Works

After comparing the results obtained with every routing paradigm, we can conclude that the differences are important when there is a significant percentage of node failures. Thus, while the average delay goes up with the number of sensors in directed diffusion and EAR, it maintains a low level of delay in SIR. The cause of this effect can be found in the fact that while directed diffusion and EAR elect the intermediate nodes using rules based on the propagation of the interest, SIR elects the intermediate nodes running an AI-algorithm. Thus, the path created by SIR avoids the election of intermediate nodes that are prone to failure because of battery draining, interference or noisy environment. Furthermore, the average dissipated energy is less in SIR when the number of nodes in the sensor goes up. We again find the reason in the effect of the election of the intermediate nodes in SIR. The use of AI in every sensor dynamically varies the assignment of this node role, distributing the energy consumption through the network. When the number of nodes is increased, the number of possible paths is increased too. Furthermore, when the percentage of node failures goes up (from 20 % to 40 %) SIR becomes the best suited protocol for these kinds of scenarios.

Although the results obtained with the inclusion of AI techniques in WSN are important and encouraging, we must take in account some relevant remarks:

– What is the price WSNs have to pay for introducing AI techniques? Although the computational payment for implementing the neural network in a sensor is inapreciable, the tradeoff associated with this implementation is the increase of the overhead. However, in typical SCADA applications, WSNs

don't have to attend high level of data traffic. Consequently, the network can support an increase on the overhead.
- Nodes failures can be provoked by the following reasons:
  - Sensor battery draining.
  - Noise originating at industrial environments.
  - Interference in the sensor surroundings.

  These phenomena provoke an influence on the average dissipated energy.

SIR has been presented in this paper as an innovative QoS-driven routing algorithm based on artificial intelligence. This routing protocol can be used over wireless sensor networks standard protocols, such as IEEE 802.15.4 and Bluetooth®, and over other well known protocols such as *Arachne*, SMACS, PicoRadio, etc.

The inclusion of AI techniques (e.g. neural networks) in wireless sensor networks has been proved to be an useful tool to improve network performances.

The great effort made to implement a SOM algorithm inside a sensor node means that the use of artificial intelligence techniques can improve the WSN performance. According to this idea, we are working on the design of new protocols using these kinds of tools.

References

1. E. Çayirci, T. Çöplü, and O. Emiroğlu. Power aware many to many routing in wireless sensor and actuator networks. In E. Çayircy, Ş. Baydere, and P. Havinga, editors, *Proceedings of the Second Europen Workshop on Wireless Sensor Networks*, pages 236–245, Istanbul, Turkey, February 2005. IEEE, IEEE Press.
2. I.F. Akyildiz, Y. Su, W. Sankarasubramaniam, and E. Çayirci. Wireless sensor networks: A survey. *Computer Networks, Elsevier*, 38:393–422, December 2002.
3. H. Karl and A. Willig. A short survey of wireless sensor networks. TKN, Technical Report Series, Berlin, October 2003.
4. K. Aspnes, D. Goldenberg, and Y. Yang. On the computational complexity of sensor network location. *Lectune Notes In Computer Science, Springer Verlag*, 3121:235–246, July 2004.
5. S. Saginbekov and I. Korpeoglu. An energy efficient scatternet formation algorithm for bluetooth-based sensor networks. In E. Çayircy, Ş. Baydere, and P. Havinga, editors, *Proceedings of the Second Europen Workshop on Wireless Sensor Networks*, pages 207–216, Istanbul, Turkey, February 2005. IEEE, IEEE Press.
6. C. Intanagonwiwat, R. Govindan, and D. Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *Proceedings of ACM Mobicom 2000*, pages 56–67, Boston, MA, USA, 2000.
7. R.C. Shah and J. Rabaey. Energy aware routing for low energy ad hoc sensor networks. In *Proceeedings of IEEE WCNC*, pages 17–21, Orlando, FL, USA, 2002.
8. J. Barbancho, C. León, F.J. Molina, and A. Barbancho. SIR: A new wireless sensor network routing protocol based on artificial intelligence. *Lecture Notes in Computer Science, Springer Verlag*, 3842:271–275, January 2006.
9. B. Sabata, S. Chatterjee, M. Davis, J.J. Sydir, and T.F. Lawrence. Taxonomy for QoS specifications. In *Proceedings of the third International Workshop on Object-Oriented Real-Time Dependable Systems*, pages 100–107. IEEE, IEEE Press, 1997.

10. J. Barbancho, F.J. Molina, D. León, J. Ropero, and A. Barbancho. OLIMPO, an ad-hoc wireless sensor network simulator for public utilities applications. In E. Çayircy, Ş. Baydere, and P. Havinga, editors, *Proceedings of the Second Europen Workshop on Wireless Sensor Networks*, pages 419–424, Istanbul, Turkey, February 2005. IEEE, IEEE Press.
11. A. Bensky. *Short-range Wireless Communication. Fundamentals of RF System Design and Application.* Elsevier, second edition, Oxford, UK 2004.
12. W. R. Heinzelman, Al Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of 33rd Annu. Hawaii Int. Conf. on System Sciences*, pages 3005–3014, Hawaii, USA, 2000.

An Energy Efficient Method for Tracking Mobile Ubiquitous Robots Using Wireless Sensor Network

Hyunsook Kim[1], Jeongho Son[1], Sukgyu Lee[2], and Kijun Han[1,*]

[1] Department of Computer Engineering,
Kyungpook National University, 1370, Sangyuk-dong, Book-gu,
Daegu, Korea 702-010
{hskim, jhson}@netopia.knu.ac.kr
[2] Department of Electrical Engineering,
Yeungnam University, 214-1, Dae-dong, Gyongsan, Korea 712-749
sglee@yu.ac.kr, kjhan@knu.ac.kr

Abstract. In general, it requires lots of complicated and expensive processing functions to find the exact location of a mobile target. For example, Ubiquitous Robotic Companion (URC) system should be equipped with powerful resources or be given an aid from the external servers to find its location for itself. Sensor network that consists of inexpensive low-power sensors can provide an efficient solution to find the exact location of such a mobile target at a low price. In such applications, if all sensor nodes have to always wake up to find location of the mobile robot, we have to pay a lot of waste of resources such as battery power and channel utilization. In this paper, we propose a cheap and energy efficient location tracking method of a mobile robot by minimizing the number of sensor nodes participating in the task of target tracking.

Keywords: Wireless sensor, target tracking, prediction, ubiquitous robot.

1 Introduction

Sensor networks consist of small and inexpensive low-power sensors, which facilitate monitoring and collecting information of sensor field. The sensors are used to monitor and control the physical environments and transmit the collected information to sink along optimized routing path. Wireless sensor network applications include such as battlefield surveillance, disaster and emergency response and traffic monitoring.

The paradigm shift of robotics is motivated by ubiquitous computing and sensor network where every device should be networked; computers should be accessible at anytime and at any place; and ubiquitous devices should be provide services suitable to the specific situation. Ubiquitous Robotic Companion (URC), a 3rd generation of robotics, provides us with various services in a ubiquitous computing environment proposed as a concept that computer are embedded everywhere [1]. Since it is inherently based on ubiquitous environment with networked sensors and actuators, it can be considered as one of the most important emerging applications of sensor network.

* Correspondence author.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 356 – 366, 2006.

Fig. 1 depicts the concept of URC with sensing, processing and acting abilities in wireless sensor network to overcome the technical constraints and producing costs by utilizing sensors and remoter computer server.

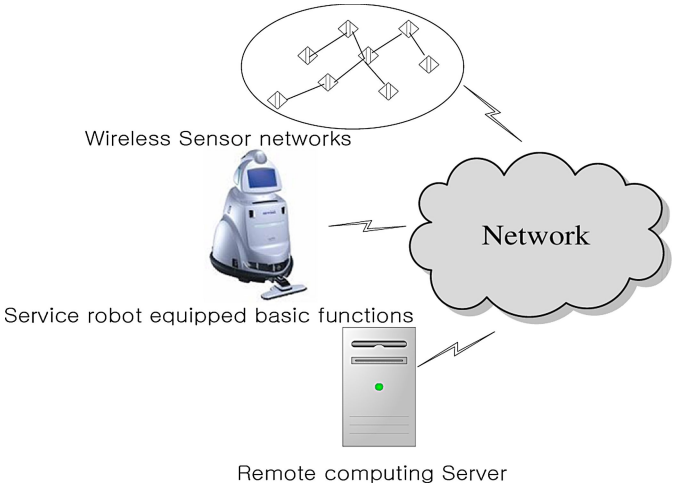


Fig. 1. The concept of the Ubiquitous Robotic Companion(URC)

By using network with external cheap sensors embedded in the environment replacing multiple robots equipped sensors, the context-awareness of the robot would be dramatically improved and lessen the burden of hardware cost [2]. In addition, remote computing server can be used as an external memory and processor of URC, which improves the robot intelligence and expands its applications and services.

URC system should be aware of its exact location at any time to perfectly carry out its mission. So, it has to be equipped with powerful resources or be given an aid from the external servers to find its location for itself since it requires lots of complicated and expensive processing functions to find its exact location. Sensor network can provide an efficient solution to find the exact location of such a mobile target at a low price. In such applications, if all sensor nodes have to always wake up to find location of the mobile robot, we have to pay a lot of waste of resources such as battery power and channel utilization.

Deciding the location of the mobile robot does not need all sensor nodes to work together. Instead, it is desirable that only several nodes surrounding the mobile robot should be responsible for observing the target to save the energy consumption and extend the network lifetime. In this paper, we propose a cheap and energy efficient location tracking method of a mobile robot by minimizing the number of sensor nodes participating in the task of target tracking. Our tracking method predicts the location of the mobile target in 2-dimensional wireless sensor network, based on linear estimation.

The rest of this paper is organized as follows. Section 2 summarizes the related works. The detailed of the proposed scheme is presented in section 3. Next, in section 4, we present some simulation results. Finally, section 5 concludes the paper.

2 Related Works

2.1 Localization

It is fundamental to know the location of robots for performing their missions, so called localization. Sensor network may play an important role to enhance the resolution of location of URC by analyzing information on locations from sensors, for which some forms of communication between reference and the receiver are needed. Some typical examples of communication technologies in sensor network include RF-based, and acoustic based communication. In RF-based localization system, distance is estimated based on received signal strength. Since RF is sensitive to noise, Cricket uses both concurrent radio and ultrasonic sounds to enhance the resolution of distance estimation. Niculescu et. al proposed a technique based on angle-of-arrival and its enhanced version, range-free techniques to estimate position. A straightforward localization approach would make use of Global Positioning System (GPS). Existing research projects such as zebra-net uses a GPS based localization, where mobile sensors find out their location every three minutes. However, the positioning systems based on GPS alone face great problems in the so-called urban canyon environments, where GPS signals are often blocked by highrise buildings and there are not enough available satellite signals to estimate the positioning information of a fix. Bulusu et. al studied signal strength based and connectivity based techniques for localization in outdoor environments. Recently Kumar et. al proposed using dead reckoning-based location services for mobile ad hoc networks [3].

2.2 Sensor Network in URC System

When a mobile robot moves around far away from the sensing range of a certain node, the nods does not need to keep wake up for participating in tracking of the mobile robot. This raises the necessity for prediction of the moving path of the mobile robot to maintain the number of participating nodes in tracking as small as possible. Many tracking protocols in large-scale sensor networks have been proposed an energy efficient tracking scheme from various angles [4] [5] [6]. Krishnamurthy *et al*. [7] [8] proposed an energy efficient technique for using a sleep schedule where the nodes go to the sleep state when there is no need to take part in sensing. In [9], they explored a localized prediction approach to power efficient object tracking by putting unnecessary sensors in sleep mode. They proposed a convey tree for object tracking using data aggregation to reduce energy consumption. In [5], they attempt to solve the problem of energy savings based on the estimating the location of a mobile target. And they studied the frequency of tracking. We apply above sleep scheduling mechanisms to our study basically.

Actually, power conservation is one of the most critical issues in wireless sensor networks since the sensor nodes that are once deployed in the sensor field would be difficult to replace a battery. With rapid advances in sensor fabrications, recent sensors are designed to be power-aware, changing their condition (e.g., shut down sensing processor or radio) when they do not need to run the components to perform a given task in a sensor field. Most sensors can operate under the three different conditions: Active, Idle and Sleep. It is important to completely shut down the radio rather

than put it in the idle mode when it does not sensing. Power management of sensor components is very important because energy consumption depends on their duties. For example, the amount of energy consumption at sensor node is shown in Fig.2.

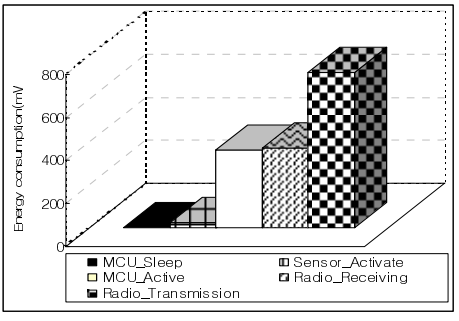


Fig. 2. Power consumption at a sensor node

So, if each node uses timely its energy to execute tasks, the network lifetime may be extended as a whole. Therefore, each sensor must minimize its battery power usage for desired longevity of network operation, which can be accomplished by properly managing sensor's operation.

3 Finding Location of URC

To save energy resources and thus extend the network lifetime, it is desirable that only several nodes surrounding the mobile robot join the task of observing the target. For example, when the target passes through the t_1 point as shown in Fig. 3, all nodes do not need to join the task for determining location and provide the results to the robot and to the external server.

Instead, it is more desirable that only several nodes around the mobile object join the task of collecting information of the robot and performing collaborative work among them. Other nodes located far from the target do not need to waste their powers to monitor the robot. If we can predict the next location of the mobile robot in advance, we can dynamically organize the group membership which should join the tracking mission. For example as shown in Fig. 3, if we predict future location of the mobile target accurately, the number of participating nodes can be minimized and thus the whole network lifetime can be extended.

As the mobile robot moves, the sensor nodes may migrate to the moving direction of the robot to keep on monitoring as shown in Fig. 3, where a thick line indicates the moving path of the mobile target and the blacked circles inside the dotted circle are tracking nodes at time t_1. Thus, sensor nodes need to control their states by themselves based on prediction of robot's movement.

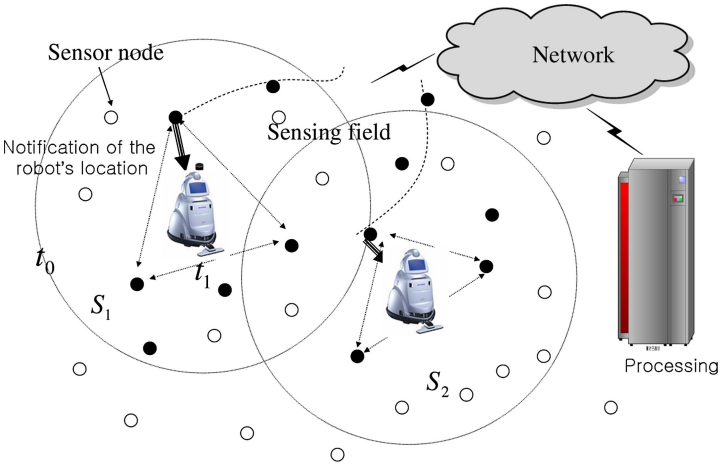


Fig. 3. Finding Location of URC in wireless sensor networks

We assume a sensor network where N sensors with the same communication and sensing range are distributed randomly in the environment that is being monitored. We also assume that each node knows its own location by using GPS or other location awareness techniques. And we utilize triangulation for localization of a mobile robot. Consequently, at least 3 sensors join the target detection and tracking with surveillance. Also each node keeps information about its neighbors such as location through the periodically message change. And each individual sensor node is equipped with appropriate sensory devices to be able to recognize the target as well as to estimate its distance based on the sensed data.

Further, we assume that we predict the location of the mobile targets every one second (or minute), and each sensor records the movement pattern of the mobile object. Basically, we use a moving average estimator to predict the future location of the mobile target based on the measurement of direction and the velocity of the mobile target.

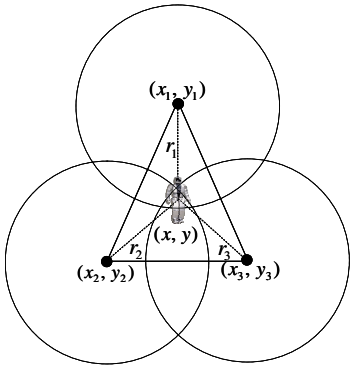


Fig. 4. Decision of location of a mobile robot using triangulation

We assume that the sensor nodes are deployed randomly in a sensor field and each sensor senses the environment and communicates its readings to the server periodically; the server triangulates the location of the object using the readings [19].

Consider three sensors whose locations $((x_1, y_1), (x_2, y_2), (x_3, y_3))$ are known. We then have

$$\begin{cases} (x-x_1)^2 + (y-y_1)^2 = r_1^2 \\ (x-x_2)^2 + (y-y_2)^2 = r_2^2 \\ (x-x_3)^2 + (y-y_3)^2 = r_3^2 \end{cases} \quad (1)$$

where r is the Euclidean distance between the robot and a sensor node. This relation is the basic equation used in triangulation.

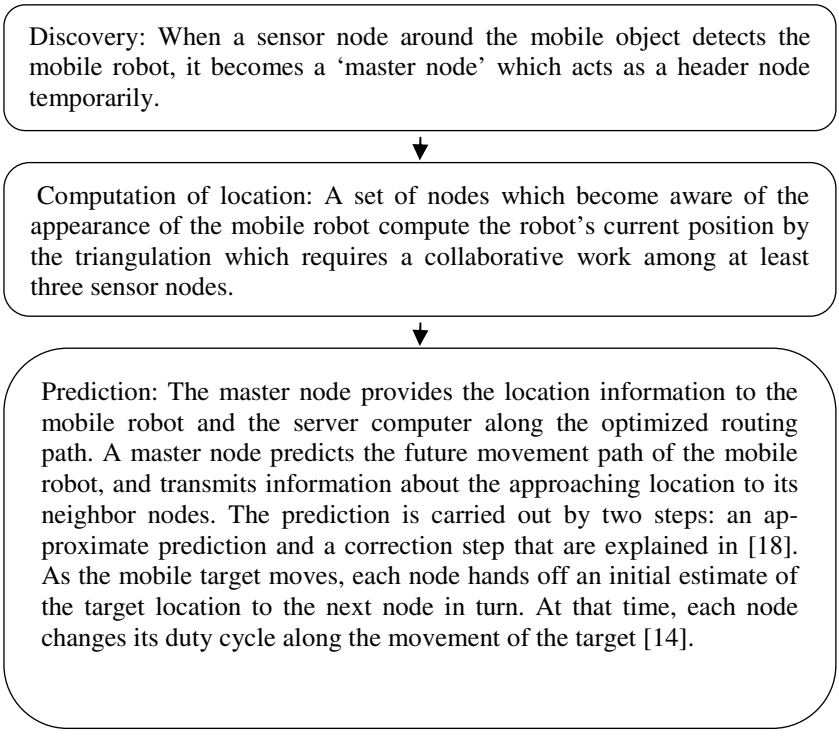


Fig. 5. Tracking procedure of the mobile robot

Solving for x and y, we get

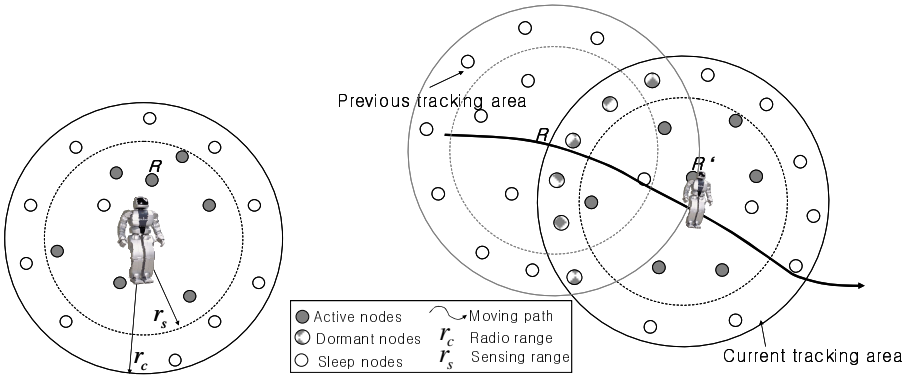
$$x = \frac{-b_2c_1 + b_1c_2}{b_2a_1 - b_1a_2}$$
$$y = \frac{-a_2c_1 + a_1c_2}{a_2b_1 - a_1b_2} \quad (2)$$

where

$$a_1 = 2(x_2 - x_1)\ ,\ b_1 = 2(y_2 - y_1)\ ,\ c_1 = x_1^2 - x_2^2 + y_1^2 - y_2^2 - r_1^2 - r_2^2\ ,$$
$$a_2 = 2\,(x_3 - x_2)\,,\ b_1 = 2\,(y_3 - y_2)\ \ ,\ \ c_1 = x_2^2 - x_3^2 + y_2^2 - y_3^2 - r_2^2 - r_3^2 \tag{3}$$

Tracking in our system is performed by the following procedure.

For energy saving, each node operates the state scheduling by itself. For example, detectable nodes within sensing range of a node '*R*' in Fig. 6, which is near the target are activated, and they are participated in tracking including localization, monitoring, and prediction.



(a) Before moving (b) After moving

Fig. 6. Change of state as the mobile target moves

So they consume amount of energy i.e., processor and sensor activating, transmitting and receiving. And the dormant node '*R*'' can hear message about appearances of the mobile target in neighborhood, but cannot detect the target since the sensing range differs from its communication range. Obviously, all dormant nodes do not need to be activated. Energy consumed by the dormant nodes is small enough to be negligible comparing with that by the activated nodes. Some nodes those are located around the next position of the target wait for sensing. The others shut down the radio after hearing the message from the master node and they wake up from sleep when their duty cycle is over. When it wakes up, it first senses its region and hears message. If a sensor node cannot detect the target and does not receive any message for target appearance, it turns off its radio and goes to sleep for saving energy. And the rest of the sensor nodes run independently according to their duty cycles. Thus, the prediction of the mobile target in the tracking system reduces energy consumption in each node and extends network lifetime.

4 Simulation

We evaluate the performance of our method through simulation results. We carry out experiments to measure missing rate and wasted energy. The network dimension for our experiments is [200, 200] and 500 nodes are randomly deployed within the region. And we assume that the sensing range of a sensor node is 20 and communication range is 35. To model the movement behavior of the mobile target, we use the Random Way Point model (RWP) and Gauss-Markov mobility model. RWP is a simple mobility model based on random directions and speeds. The mobile object begins by staying in one location for a certain period of time. Once this time expires, the mobile object chooses a random destination in the field and a speed. And then travels toward the newly chosen destination at the selected speed. Upon arrival, the mobile object pauses for a specified time period before starting the process again. Gauss-Markov Mobility Model is a model that uses one tuning (α) parameter to vary the degree of randomness in the mobility pattern. Initially, each mobile node is assigned a current speed and direction. Specifically, the value of speed and direction at the n^{th} instance is calculated based upon the value of speed and direction at the $(n-1)^{th}$ instance and a random variable [15]. Energy consumption used for simulation is based on some numeric parameters obtained in [5].

Our prediction method is compared with the *least squares minimization* (LSQ) to evaluate the performance of accuracy. LSQ is a common method used for error reduction in estimation and prediction methods. LSQ solves the problem of estimating by minimizing the sum of the squares of the error terms corresponding to each distance sample. In other words, LSQ tries to get the estimate by minimizing $\sum_{i=1}^{n}(\|\hat{\phi}_i - p_i\| - d_i)^2$ where $\hat{\phi}_n$ is estimate and $\|\hat{\phi}_i - p_i\|$ is the Euclidean distance between the estimated coordinate of the mobile device and the beacon or receiver at position p_i [16].

4.1 Energy

Fig. 7 shows the wasted energy that is defined as the amount of consumed power due to incorrect information of prediction over all nodes. Obviously energy consumption is greatly influenced by an accuracy of prediction. If the sensor nodes stay awake to track the mobile robot while the robot is moving out of the sensing range, they consume unnecessary energy. As described earlier, we can extend the network lifetime by avoiding such unnecessary energy consumption at nodes that do not need to join in tracking. This figure indicates that our scheme can decrease the number of participating nodes and thus reduce energy consumption too.

4.2 Participating Nodes

We first examine the number of detectable nodes in the sensing field. We can roughly compute the number of participation nodes to be involved in a mobile robot detection at a given time *t* by

$$S_t = \frac{N \ \pi \ r_s^2}{A} \tag{4}$$

where N is the number of deploying nodes in whole sensor field A and r_s is the sensing range of the node. Fig. 8 shows percentage of the number of nodes that are able to detect the mobile target as varying the sensing range of the node.

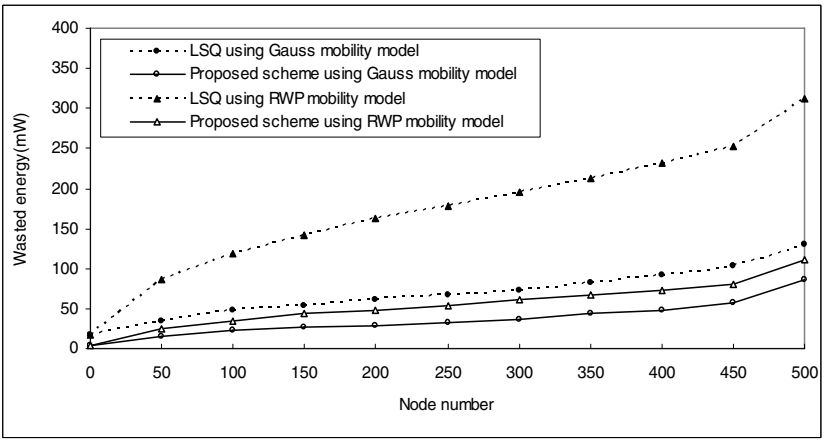


Fig. 7. Unnecessary waste of energy

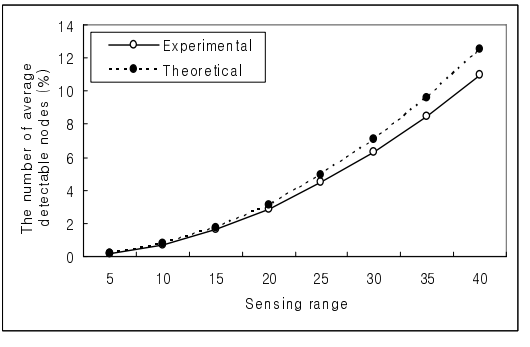


Fig. 8. Number of detectable nodes as the sensing range of node is varied

We can see that there is a sound agreement between the theoretical and experimental values. This figure also indicates we can reduce energy consumption considerably by allowing only some nodes around the mobile target to join in the tracking.

4.3 Exposed Time

Fig. 9 shows the percentage of the time duration when the location of the mobile robot can be known to any three or more nodes in the network. We call this exposed

time. As previously mentioned, at least three nodes are needed simultaneously to decide the location of the target using triangulation. From this figure, we can see that the target is always detected by three sensor nodes regardless of location of the mobile target when sensing range is greater than 20.

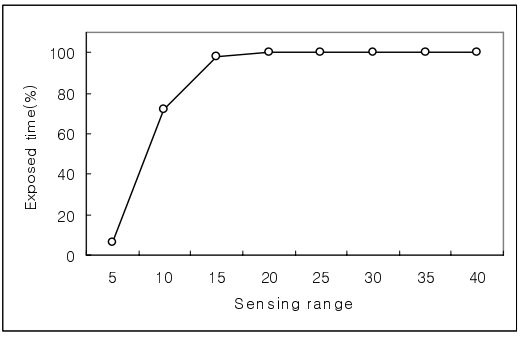


Fig. 9. Exposed time of target as the sensing range of node is varied

5 Conclusion

In this paper, we propose a cheap and energy efficient location tracking method of a mobile URC using a sensor network. Our method relieves the URC from the burden of complicated processing and computation to find its exact location by allowing only several nodes around the mobile URC to join the mission of location tracking. Our tracking method is based on a moving average estimator and simulations results show that our proposal can be successfully applicable to finding the location of mobile URC.

References

1. S.R. Oh, "IT Based Intelligent Service Robot," In *Proceeding of the First NSF PI Workshop on Robotics and Computer Vision(RCV '03)*, Las Vegas, Oct. 2003.
2. H. Kim, Y.-J. Cho and S.-R. Oh, "CAMUS: A middleware supporting context-aware services for network-based robots," In *Proceeding of the IEEE Workshop on Advanced Robotics and its Social Impacts(ARSO)* , 2005.
3. Sameer Tilak, Vinay Kolar, Nael B. Abu-Ghazaleh and Kyoun-Dong Kang, "Dynamic Localization Protocols for Mobile Sensor Networks", In *Proceeding of the IEEE IWSEEASN,* 2005.
4. C. Gui and P. Mohapatra, "Power conservation and quality of surveillance in target tracking sensor networks," In *Proceeding of the ACM MobiCom,* 2004.
5. Y. Xu, J. Winter, and W.-C. Lee, "Prediction-based strategies for energy saving in object tracking sensor networks," In *Proceeding of IEEE International Conference on Mobile Data Management(MDM),* 2004.
6. D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," In *Proceeding of the ACM/IEEE International Conference on Mobile Computing and Networking*, 1999.

7. T.Yan, T,He, and J, Stankovic , "Differentiated surveillance for sensor networks," In *Proceeding of ACM SenSys'03,* 2003.
8. T. He, S. Krishnamurthy, J. Stankovic, T. Abdelzaher, L. Luo, R. Storelu, T. Yan, L. Gu, J. Hui, and B.Krogh, "Energy-efficient surveillance system using wireless sensor networks," In *Proceeding of the MobiSYS'04*, 2004.
9. Y.Xu and W.-C.Lee, "On Localized Prediction for Power Efficient Object Tracking in Sensor Networks," In *Proceeding of the Intionational Workshop on Mobile Distributed Computing(MDC*), 2003.
10. R. Brooks and C. Griffin, "Traffic model evaluation of ad hoc target tracking algorithms," In *Proceeding of the International Journal of High Performance Computer Applications*, 2002.
11. R. Brooks and C. Griffin and D. S. Friedlander, "Self-organized distributed sensor networks entity tracking," In *Proceeding of the International Journal of High Performance Computer Applications*, 2002.
12. D. Li, K. Wong, Y.Hu and A. Sayeed, "Detection, Classification, Tracking of Targets in Micro-sensor Networks," In *Proceeding of the IEEE Signal Processing Magazine,* pp. 17-29, March 2002.
13. S. Goel and T. Imielinski, "Prediction-based monitoring in sensor networks: tasking lessons from MPEG," In *Proceeding of the ACM Computer Communication Review*, 2001.
14. F. Zhao, J. Liu, J. J. Liu, L. Guibas, and J. Reich, "Collaborative signal and information processing: An information directed approach," In *Proceeding of the IEEE,* 2003.
15. T. Camp, J. Boleng and V. Davies, "A survey of mobility models for ad hoc network research," In *Proceeding of the Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking*, 2002.
16. A. Smith, H. Balakrishnan, M. Goraczko and N. Priyantha, "Tracking Moving Devices with the Cricket Location Systems," In *Proceeding of the Mobisys,* 2004.
17. H. Yang and B. Sikdar, "A Protocol for Tracking Mobile Targets using Sensor Networks," In *Proceeding of the IEEE Workshop Sensor Network Protocols and Applications, (in conjunction with IEEE ICC)*, May, 2003.
18. HS. Kim, KJ. Han "An Energy Efficient Tracking Method in Wireless Sensor Networks", In *Proceeding of the 6th Next Generation Teletraffic and Wired/Wireless Advanced Networks(NEW2AN)*, May, 2006.
19. Xingbo Yu, Koushik Niyogi, Sharad Mehrotra, Nalini Venkatasubramanian, "Adaptive Target Tracking in Sensor Networks," In *Proceeding of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS'04),* 2004.

LSec: Lightweight Security Protocol for Distributed Wireless Sensor Network*

Riaz Ahmed Shaikh, Sungyoung Lee, Mohammad A.U. Khan, and Young Jae Song

Department of Computer Engineering, Kyung Hee University,
Sochen-ri, Giheung-eup, Yongin-si, Gyeonggi-do, 449-701, South Korea
{riaz, sylee, khan}@oslab.khu.ac.kr, yjsong@khu.ac.kr

Abstract. Constraint specific wireless sensor networks need energy efficient and secure communication mechanisms. In this paper we propose Lightweight Security protocol (LSec) that fulfils both requirements. LSec provides authentication and authorization of sensor nodes with simple secure key exchange scheme. It also provides confidentiality of data and protection mechanism against intrusions and anomalies. LSec is memory efficient that requires 72 bytes of memory storage for keys. It only introduces 74.125 bytes of transmission and reception cost per connection.

1 Introduction

Wireless sensor networks consist of a large number of small size sensor nodes deployed in the observed environment. Sensor nodes have smaller memory (8K of total memory and disk space) and limited computation power (8-bit, 4 MHz CPU) [1]. They usually communicate with a powerful base station which connects sensor nodes with external networks. The limited energy at senor nodes creates hindrances in implementing complex security schemes. There are two major factors for energy consumption:

1. Transmission and reception of data.
2. Processing of query request.

Wireless networks are relatively more vulnerable to security attacks than wired networks due to the broadcast nature of communication [1]. In order to implement security mechanism in sensor networks, we need to ensure that communication overhead is less and consumes less computation power. With these constraints it is impractical to use traditional security algorithms and mechanism meant for powerful workstations.

Sensor networks are vulnerable to a variety of security threats such as DoS, eavesdropping, message replay, message modification, malicious code, etc. In order to secure sensor networks against these attacks, we need to implement message

* This work is financially supported by the Ministry of Education and Human Resources Development (MOE), the Ministry of Commerce, Industry and Energy (MOCIE) and the Ministry of Labor (MOLAB) through the fostering project of the Lab of Excellency. The corresponding author of this paper is Prof. Sungyoung Lee.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 367 – 377, 2006.

confidentiality, authentication, message integrity, intrusion detection and some other security mechanism. Encrypting communication between sensor nodes can partially solve the problems but it requires a robust key exchange and distribution scheme.

In general, there are three types of key management schemes [2,3]: Trusted Server scheme, self enforcing scheme and key-predistribution scheme. Trusted server schemes relies on a trusted base station, that is responsible for establishing the key agreement between two communicating nodes as described in [4]. It uses symmetric key cryptography for data encryption. The main advantages of this scheme are, it is memory efficient, nodes only need to store single secret key and it is resilient to node capture. But the drawback of this scheme is that it is energy expensive, it requires extra routing overhead in the sense that each node need to communicate with base station several times [3]. Self enforcing schemes use public key cryptography for communication between sensor nodes. This scheme is perfectly resilient against node capture and it is fully scalable and memory efficient. But the problem with the traditional public keys cryptography schemes such as DSA [5] or RSA [6] is the fact that they require complex and intensive computations which is not possible to perform by sensor node having limited computation power. Some researchers [7,8] uses Elliptic curve cryptography as an alternative to traditional public key systems but still not perfect for sensor networks. Third scheme is key pre-distribution scheme based on symmetric key cryptography, in which limited numbers of keys are stored on each sensor node prior to their deployment. This scheme is easy to implement and does not introduce any additional routing overhead for key exchange. The degree of resiliency of node capture is dependent on the pre-distribution scheme [3].

Quite recently some security solutions have been proposed in [9,10,11,12,13] especially for wireless sensor networks but each suffers from various limitations such as higher memory and power consumptions that are discussed in section 4.

Keeping all these factors in mind we propose a lightweight security protocol (LSec) for wireless sensor networks. LSec combines the features of trusted server scheme and Self Enforcing security schemes. Our main contribution is the designing and implementation of LSec that provides

- Authentication and Authorization of sensor node.
- Simple Secure key exchange scheme.
- Secure defense mechanism against anomalies and intrusions.
- Confidentiality of data.
- Usage of both symmetric and asymmetric schemes.

The rest of the paper is organized as follows. Section 2 describes the details of LSec. Section 3 presents the simulation results and evaluation of LSec. Section 4 presents the comparison of LSec with other security solutions and Section 5 consists of conclusion and future direction.

2 Light Weight Security Protocol (LSec)

The basic objective of LSec is to provide lightweight security solution for wireless sensor networks where all nodes can communicate with each other. LSec can support both static and mobile environment, which may contain single and multiple Base

Stations (BS). Basic system architecture is shown in figure 1. LSec uses both symmetric and asymmetric schemes for providing secure communication in wireless sensor networks.

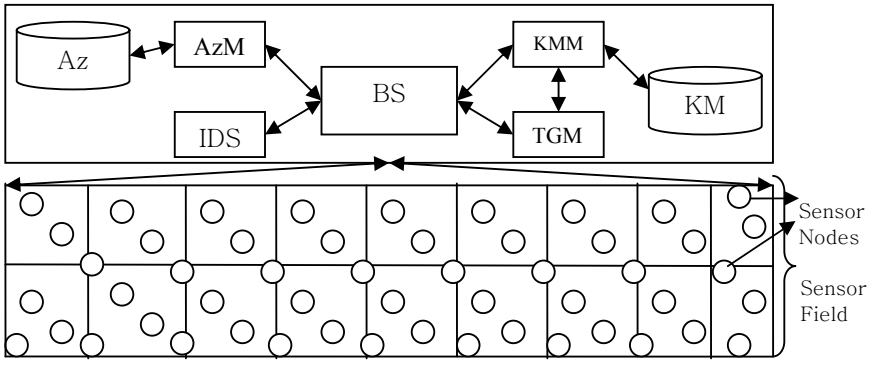


Fig. 1. LSec System Architecture

Key Management Module (KMM) is used to store public and shared secret key of each node with BS to the database. Token Generator Module (TGM) is used to generate the tokens for the requesters, which will be further used by the other communicating party for the authentication of requester node. Authorization Module (AzM) is used to check whether a particular node is allowed to communicate with other node or group. Lightweight mobile agents will only be installed on Cluster heads which sends alerts messages to intrusion detection system (IDS), which is responsible for detecting any anomaly or intrusion in the network. Basic assumptions and rules of LSec are given below.

2.1 Assumptions

1. Base Station (BS) is the trusted party and it will never be compromised. Compromising the Base station can render the entire sensor network useless, and it is the only point from where sensor node can communicate with external networks.
2. Only Base Station (BS) knows the Public keys (Pk) of all the sensor nodes in the network. Communicating nodes will know each other's public key during the time of connection establishment.

2.2 Rules

- Asymmetric scheme will only be used for sharing ephemeral secret key between communicating nodes.
- For every session new random secret key will be used.
- Data will be encrypted by using symmetric schemes because these schemes are considered to be executed three to four times faster than asymmetric schemes [14].

2.3 LSec Packet Format

LSec packet format is shown in table 1. Currently LSec uses seven types of packets, 'Request', 'Response', 'Init', 'Ack', 'Data', 'Update Group Key' and 'Alert' packet. All seven packets are distinguished by 'type' field in the LSec packet. IDsrc field contain the id of sending node and last encrypted portion contain the information depending upon the type of packet, as shown in table 1.

Table 1. LSec: Type field

Type	ID_{src}	Encrypted Portion
Request	Any (sensor node)	$EK_{A\text{-}BS}$ (Intended-ID_{dest} , N)
Response	BS	$EK_{A\text{-}BS}$ (R-type, Intended-ID_{dest} , N , Pk, token | R)
Init	Any (sensor node)	EK_B^+(N, Pk, token)
Ack	Any (sensor node)	EK_A^+(N,sk)
Data	Any (sensor node)	EKsk (data)
UpdateGroupKey	Any CH sensor node	EK_G (GroupID, new Key), MAC
Alert	Any CH sensor node	$EK_{CH\text{-}BS}$ (Alert-type), MAC

$EK_{A\text{-}BS}$ = Encrypt with the secret key shared between node A and BS
EK_A^+ = Encrypt with the public key of node A
EK_B^+ = Encrypt with the public key of node B
EK_{sk} = Encrypt with the shared secret key
EK_G = Encrypt with group key
$EK_{CH\text{-}BS}$ = Encrypt with the secret key shared between Cluster head and BS
R-type = Response type (positive or negative response)
R = Reason of negative acknowledgement
Intended-ID_{dest} = ID of Intended Destination
Pk = public key
ID_{src} = ID of source node
N = Nonce (Unique Random Number)
MAC = Message Authentication Code
CH = Cluster Head

The distribution of bits to different fields (as shown in table 2), introduces some upper limits, such as, size of source address is of 2 bytes, it means our LSec works only in the environment where number of sensor nodes not exceeding 2^{16}. Length of Nonce (unique random number) field is of 3 bytes, so LSec can allow maximum of 2^{24} connections at a time. The length of public key and private key is of exactly 128

Table 2. Distribution of bits to different fields of LSec

Field	Size	Field	Size
Type	4 bits	Public and Private key	128 bits
IDsrc, IDdest	16 bits	Secret key	64 bits
Nonce (N)	23 bits	token	4 bytes
R-type	1 bit	data	30 bytes

bits and the length of secret key is of exactly 64 bits. Only stream cipher encryption algorithms are allowed to use because of a fixed length size of packets. MAC is of 64 bits.

2.4 Procedure

LSec works in three phases, authentication and authorization phase, key distribution phase, and data transmission phase. Authentication and authorization is performed during the exchange of "Request" and "Response" packet by using symmetric scheme. Key distribution phase involves sharing of random secret key in a secure manner by using asymmetric scheme. In this phase "INIT" and "ACK" packets will be exchanged. Data transmission phase involves transmission of data packet in an encrypted manner.

Let's suppose node A wants to communicate with the node B. It will first send request packet to Base station, for receiving token and public key of node B. The request packet is encrypted with the secret key shared between node A and BS. BS first checks in the database via AzM that weather node A has rights to establish connection with node B. If yes, it generates the token which will be further used by the node B for the authentication of node A. That token is encrypted with secret key shared between node B and BS, so that node A will not able to decrypt token. BS will sent back a response packet that contains token, public key of node B and Nonce (Unique Random Number) that was there in request packet. Nonce will ensure node A that packet came from genuine BS. When node A gets the positive response from BS it sent the INIT packet to node B that contains Nonce, its own public key and token generated by BS. The whole INIT packet is encrypted with the public key of node B. When node B gets INIT packet it first check token, if it is correct, it will generate the secret key and sent it back to node A in an encrypted manner. When node A gets ACK packet, it deletes the public key of node B from its memory, and sent data to node B by using new session secret key. When data transmission complete, both nodes delete that session key. For group communication, each node uses the group secret key for data transmission in a secure manner. Cluster head will update this key after periodic interval.

3 Simulation and Performance Analysis

We have tested our LSec protocol on Sensor Network Simulator and Emulator (SENSE) [15]. In sensor node we introduce the middleware between application layer and network layer as shown in figure 2.

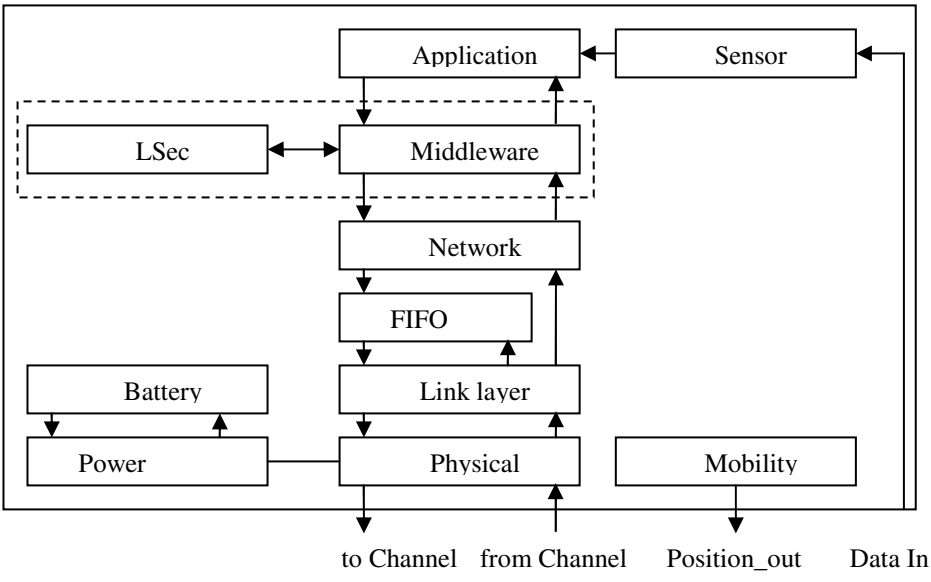


Fig 2. Sensor Node Architecture

Table 3. Simulation Parameters

Terrain	1000x1000
Total Number of Nodes	101 (including BS)
Initial battery of each sensor node	$1x10^6$J
Power consumption for transmission	1.6W
Power consumption for reception	1.2 W
Idle power consumption	1.15W
Carrier sense threshold	3.652e-10W
Receive power threshold	1.559e-11W
Frequency	9.14e8
Transmitting & Receiving antenna gain	1.0

That middleware uses LSec for the enforcement of security in the sensor network. At application layer we use constant bit rate component (CBR) that generate constant traffic during simulation between two communicating sensor nodes. For the demonstration and performance evaluation of LSec, CBR is run with and without

LSec. We randomly deploy 100 sensor nodes plus one Base station (BS) in 1000 by 1000 terrain. Basic simulation parameters employed are described in table 3.

3.1 Performance Analysis of Communication Overhead

In our simulation scenario, application sent data packets of size 30 bytes in a periodic interval. The overall communication overhead of LSec for one to one communication is decreases with the increase in transfer of number of data packets as shown in figure 3. Communication Overhead (C0 %) is calculated as

$$CO(\%) = \left(\frac{Nc * 74.125}{\sum_{i=1}^{n} N_i^P * 30}\right) * 100 \tag{1}$$

Where as 'Nc' is the total number of connections. N_i^P is the number of packets transferred by node i. We multiplied 74.125 bytes to Nc because for every connection LSec exchange four control packets (Request, Response, Init, and Ack) during the authentication, authorization and key exchange phase whose cumulative size is 74.125 byte. Size of each data packet is 30 bytes.

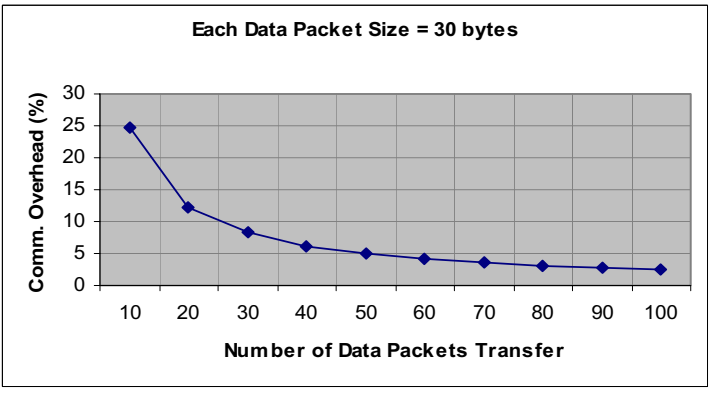


Fig. 3. Communication Overhead (%) of LSec

3.2 Performance Analysis of Power Computation

Power Computation primarily depends upon the kind of symmetric and asymmetric scheme. If we assume that computation power required for symmetric encryption and decryption scheme is CSE and CSD respectively and computation power of asymmetric encryption and decryption scheme as CAE and CAD respectively. Then the total power consumption required by single node during first two phases is

$$Power\ Computation = (CSE + CSD) + (CAE + CAD) \tag{2}$$

Computation power required by a single node during data transmission phase is calculate as,

$$Power\ Computation = (TNSP*CSE) + (TNRP*CSD) \quad (3)$$

Where TNSP is the Total Number of Sent data packets and TNRP is the Total Number of received data packets.

3.3 Performance Analysis of Memory Consumption

Every sensor node needs to store only six keys, three of them are permanent and three are ephemerals. Permanent keys consist of one public key (self), one private keys and one public key of BS. Ephemerals keys consist of group key, public key of other node and session secret key. In order to save these keys only 72 bytes are needed. Details are given in table 4. This approach will make sensor network memory efficient.

Table 4. Storage Requirement of Keys

S/No	Keys	Size (in bytes)
Permanent Keys		
1	Public key of node	16
2	Private key of node	16
3	shared secret key b/w Node & BS	8
Ephemeral Keys		
4	Group Key	8
5	Public key of other node	16
6	Session key	8
Total Storage size Required		72 bytes

3.4 Performance Analysis of Energy Consumption

The main source of energy consumption at sensor node is its transmission and reception cost. We used SENSE that consumes energy in four different modes: TRANSMIT, RECIEVE, IDLE, and SLEEP. Energy consumption rate of each mode

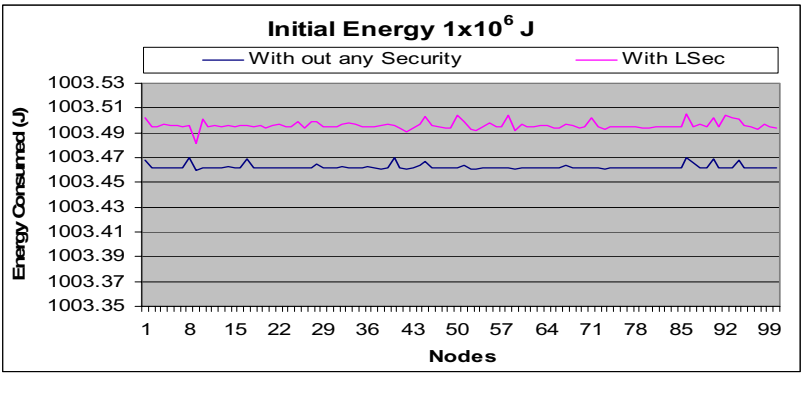


Fig 4. Energy Consumptions

is given in table 3. For each connection, LSec exchange four control packets (Request, Response, Init, and Ack) of cumulative size 74.125 bytes that requires for authentication, authorization and key exchange mechanism. That is an acceptable tradeoff between energy and security. Simulation result of energy consumption is shown in figure 4.

3.5 Resilience Against Node Compromise

Single node compromised will not expose the whole communication in network. Only the communication links that are established with compromised node will expose the network. Let's suppose 'Ncn' is the set of nodes that establish connections and 'Ncp' is the set of compromised nodes. Then Ncn ∩ Ncp will give us the set of nodes that are compromised as well as connected. Then the maximum number of connections that can be exposed only if all compromised nodes connected to uncompromised nodes. On the other hand minimum numbers of links that can be exposed only if all compromised nodes are connected with each other.

$$Max : Ncn \bigcap Ncp \tag{4}$$

$$Min : \begin{cases} \dfrac{Ncn \bigcap Ncp}{2} & for \longrightarrow even \\ \left(\dfrac{Ncn \bigcap Ncp + 1}{2}\right) & for \longrightarrow odd \end{cases} \tag{5}$$

If we assume that sensor networks consists of 1000 nodes and total 500 connections established between pair of nodes then the total links that can be minimum and maximum compromised is shown in figure 5.

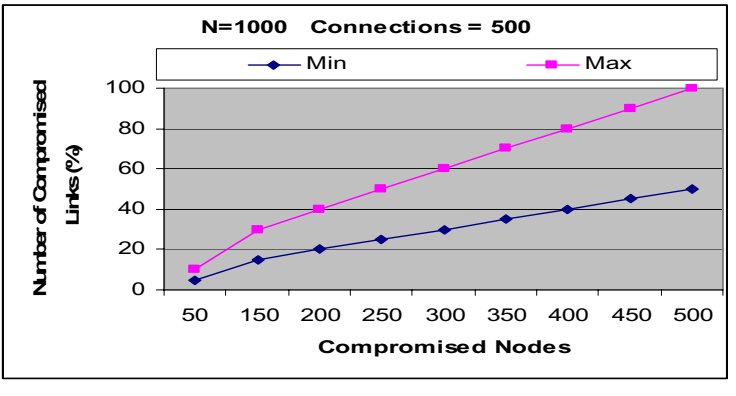


Fig. 5. Percentage of Compromised Links

4 Comparison of LSec with Other Security Solutions

Comparison of all above discussed schemes with LSec is given in table 5. We provided comparison from the perspective of memory requirement, transmission cost,

and some other basic security parameters such as authentication, authorization, confidentiality, etc. Data integrity is generally handled at link layer with the help of some hashing schemes such as MD5, SHA1 etc or by CRC schemes and availability is normally handled at physical layer. LSec lies between network and application layer that's why it doesn't provide explicit data integrity and availability support.

Table 5. Comparison of LSec with other security solutions

		SPINS	TinySec	LiSP	LSec
Memory Requirement with respect to storage of keys		3	Depended on KMS[1]	≥ 8	6
Cost Transmission	During key exchange (bytes)	--	Depended on KMS	12.6*TNN[2]	74.125*TNC[3]
	During Data Transmission	20%	10%	> 20	8.33%
Public Key Cryptography Support		No	No	No	Yes
Symmetric key cryptography Support		Yes	Yes	Yes	Yes
Intrusion Detection mechanism		No	No	Yes	Yes
Authentication support		Yes	Yes	Yes	Yes
Authorization support		No	No	Yes	Yes
Data Integrity support		Yes	Yes	Yes	No
Confidentiality support		Yes	Yes	Yes	Yes
Availability support		No	No	Yes	No

[1] KMS: Key Management Scheme
[2] KNN: Total Number of Nodes
[3] KNC: Total Number of Connections

5 Conclusion and Future Directions

We proposed Lightweight security protocol (LSec) for wireless sensor networks, which provides authentication and authorization of sensor node. It also provides

simple secure key exchange scheme and confidentiality of data. LSec is highly scalable and memory efficient. It uses 6 keys, which takes only 72 bytes of memory storage. It introduces 74.125 bytes of transmission and reception cost per connection. It has the advantage of simple secure defense mechanism against compromised nodes. In future, we will try to solve the issue related to the neighboring nodes of the base station that suffered from higher communication overhead by forwarding request and response packets during authentication and authorization phase.

References

1. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *proc. of the First IEEE International Workshop on Sensor Network Protocols and Applications (WSNA'03)*, May 2003, pp. 113- 127
2. Wenliang Du, Jing Deng, Han, Y.S., Shigang Chen, Varshney P.K, "A key management scheme for wireless sensor networks using deployment knowledge", *proc. of INFOCOM 2004*, Mar 2004
3. Lydia Ray, "Active Security Mechanisms for Wireless Sensor Networks and Energy optimization for passive security Routing", *PhD Dissertation*, Dep. of Computer Science, Louisiana State University, Aug 2005
4. J. Kohl and B. Clifford Neuman, "The Kerberos Network Authentication Service (v5)", RFC 1510, Sep 1993
5. W. Diffie and M.E. Hellman, "New Directions in Cryptography", *IEEE Transaction on Information Theory*, vol. 22, Nov 1976, pp. 644-654.
6. R. L. Rivest, A. Shamir, L.M. Adleman, "A method for obtaining Digital Signatures and Public key cryptosystem", *Communication of ACM*, vol. 21(2), 1978, pp. 120-126
7. Erik-Oliver Blaß and Martina Zitterbart, "Towards Acceptable Public-Key Encryption in Sensor Networks", *proc. of 2nd International Workshop on Ubiquitous Computing, ACM SIGMIS*, May 2005
8. John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless sensor network security: A Survey", *Technical Report MIST-TR-2005-007*, July, 2005
9. A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security protocols for sensor networks", *proc. of 7th annual international conference on Mobile computing and networking*, Rome, Italy, Aug 2001, pp 188-189
10. Chris Karlof, Naveen Sastry, and David Wagner, "TinySec: a link layer security architecture for wireless sensor networks", *Proc. of the 2nd international conference on Embedded networked sensor systems*, Baltimore, MD, USA, Nov 2004, pp 162-175
11. K. Jones, A.Wadaa, S. Oladu, L. W|son, and M. Etoweissy, "Towards a new paradigm for securing wireless sensor networks", *proc. of the 2003 workshop on New security paradigms*, Ascona, Switzerland, Aug 2003, pp 115 - 121
12. Taejoon Park, and Kang G. Shin, "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks", *ACM Transactions on Embedded Computing Systems*, vol. 3(3), Aug 2004, pp. 634–660
13. Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: Efficient Security Mechanism for Large-Scale Distributed Sensor Networks ", *Proc. of the 10th ACM conference on Computer and communications security*, Washington, USA, 2003, pp. 62-72
14. Elaine Shi and Adrian Perrig, "Designing Secure Sensor Networks", *IEEE Wireless Communications*, Dec 2004, pp. 38-43
15. Sensor Network Simulator and Emulator (SENSE) http://www.cs.rpi.edu/~cheng3/sense/

Design of New Concatenated Space-Time Block Codes Using Odd Transmit Antennas

Taejin Jung[1] and Wangrok Oh[2,⋆]

[1] Dept. of Electronics and Computer Eng., Chonnam National University,
300 Yongbong-dong, Puk-gu, Kwangju, 500-757, Korea
tjjung@chonnam.ac.kr
[2] Div. of Electrical and Computer Eng., Chungnam National University,
220 Gung-dong, Yuseong-gu, Daejeon, 305-764, Korea
kingrock@cnu.ac.kr

Abstract. In this paper, a new class of space-time block codes achieving full-rate and full spatial diversity for QAM is proposed when using any odd transmit antennas over quasi-static Rayleigh fading channels. Like the conventional A-ST-CR codes [10], the proposed codes are constructed by serially concatenating the constellation-rotating precoders [7]-[9] with the Alamouti scheme [3]. Computer simulations show that for the case of QPSK, the best code in this class achieves approximately 1.5dB larger coding gain than the existing ST-CR code [8], [9] for both 3 and 5 transmit antennas at average SER=10^{-5} and for the case of 16-QAM, 3dB for 3 transmit antennas. The codes possessing quasi-orthogonal characteristic are also included in this class, allowing simple ML decoding with virtually no performance loss compared to the best code in the class.

1 Introduction

Recently, the space-time coding technique [1] using multiple transmit antennas has received considerable attention as a promising technique to enhance the capacity and quality of mobile wireless systems. Tarokh *et al.* in [2] developed orthogonal space-time block codes (O-STBCs) based on orthogonal designs achieving full diversity and allowing simple maximum likelihood (ML) decoding. Unfortunately, full-rate O-STBCs for general complex modulation such as PSK and QAM do not exist when the number of transmit antennas is larger than two [2], [3]. Yan *et al.* in [8], [9] proposed so called space-time constellation-rotating (ST-CR) codes achieving both full-rate and full spatial diversity for general QAM when using any number of transmit antennas. This is done by transmitting the precoded symbols generated by multiplying a vector of QAM symbols via linear constellation-rotating precoders. By serially concatenating these linear precoders with the Alamouti scheme [3], Jung *et al.* in [10] presented so called Alamouti ST-CR (A-ST-CR) codes enjoying larger coding gains than the ST-CR codes without any loss of code rate. However, these codes were only designed for an

⋆ Corresponding author.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 378–388, 2006.

even number of transmit antennas. Also, these two classes of codes based on the linear precoders have a great deficiency of not satisfying the Tarokh's orthogonal designs [2], resulting in a greatly higher ML decoding complexity compared to the O-STBCs.

Hence, based on the design idea in the A-ST-CR codes, we will present a new class of STBCs achieving full rate and full diversity for QAM and quasi-static Rayleigh fading channels when using any odd number of transmit antennas. These codes are designed by serially concatenating the constellation-rotating precoders with the Alamouti scheme like the conventional A-ST-CR codes. Computer simulations show that for the case of QPSK, the best code in this class achieves approximately 1.5dB larger coding gain than the existing ST-CR code for both 3 and 5 transmit antennas at average SER=10^{-5} and for the case of 16-QAM, 3dB for 3 transmit antennas. Specifically, new codes satisfying quasi-orthogonal characteristic [4]-[6] are also included in this class, exhibiting almost same error performance as the best code in the class. The quasi-orthogonal property allows a ML decoder at the receiver to decode two groups of modulated symbols separately, resulting in greatly simplified ML decoding at the receiver. The simple ML decoding algorithm based on the quasi-orthogonal characteristic will be presented in Section IV in detail.

This paper is organized as follows. In Section II, system model considered in this paper is described and in Section III, some important characteristics of the conventional ST-CR and A-ST-CR codes are briefly reviewed. Then we design the new full-rate STBCs with full diversity for odd transmit antennas in Section III and present the simulation results for these codes in Section IV. Finally, conclusions are drawn in Section V.

2 System Model

The basic system model considered in this paper is identical to that of STBC with N transmit and one receive antennas under quasi-static Rayleigh fading channels [10], which is depicted in Fig. 1.

The transmitter first groups the QAM symbols with unit energy to form vectors of length L, $\mathbf{x} = [x_1, \cdots, x_L]^T$ where $\mathbf{z}^T$ denotes the transpose vector of $\mathbf{z}$. This vector is then input to the space-time encoder to form a codeword matrix $\mathbf{S}(\mathbf{x}) = \{s_{ij}\}$ of size $T_0 \times N$. The codeword symbol s_{ij} is then transmitted on antenna j at time i. Here, we focus on STBCs achieving full rate by setting $T_0 = L$. We also normalize the codeword matrix $\mathbf{S}(\mathbf{x})$ with energy constraint $E\{\|\mathbf{S}(\mathbf{x})\|^2\} = L$ where $E\{\cdot\}$ and $\|\cdot\|$ denote the expectation operator and Frobenius norm, respectively.

The symbols transmitted from different transmit antennas are assumed to experience independent Rayleigh fading. The channel is also assumed to be quasi-static in the sense that the channel do not vary significantly during the transmission of the code matrix. Hence, a received vector $\mathbf{y} = [y_1, \cdots, y_L]^T$ with a matched filter output y_i at time i is given as

$$\mathbf{y} = \sqrt{E_s}\mathbf{S}(\mathbf{x})\mathbf{h} + \mathbf{n} \tag{1}$$

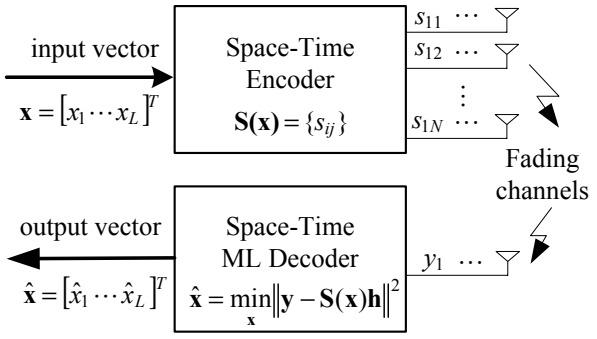


Fig. 1. System model for STBC with N transmit and one receive antennas

where E_s and $\mathbf{h} = [h_1, \cdots, h_N]^T$ denote the average received symbol energy and the channel gain vector, respectively, where h_n represents the complex channel gain between the nth transmit antenna and the receive antenna with zero mean and unit variance. Also, $\mathbf{n} = [n_1, \cdots, n_L]^T$ denotes the received noise vector of length L where n_i represents a sample of the i.i.d. complex Gaussian random variable at time i with zero mean and variance N_0.

It is assumed that the channel gain vector is perfectly known at the receiver. Using this assumption, ML decoding is performed at the receiver by choosing $\hat{\mathbf{x}}$ such that $\mathbf{S}(\hat{\mathbf{x}})\mathbf{h}$ is closest to $\mathbf{y}$ in terms of Euclidean distance given as

$$\hat{\mathbf{x}} = arg \min_{\mathbf{x}} \|\mathbf{y} - \mathbf{S}(\mathbf{x})\mathbf{h}\| . \tag{2}$$

3 Conventional ST-CR and A-ST-CR Codes

Both the conventional ST-CR [8], [9] and A-ST-CR [10] encoders with even N transmit antennas first generate a precoded vector $\mathbf{r} = [r_1, \cdots, r_N]^T$ of length N by multiplying an N dimensional input vector $\mathbf{x}$ of length N by a constellation-rotating precoder $\mathbf{\Theta}$ of size $N \times N$, i.e., $\mathbf{r} = \mathbf{\Theta}\mathbf{x}$. The ST-CR encoder transmits r_i at time i using a subgroup of the N transmit antennas so as to guarantee that the symbol r_i experiences independent fading. But, the A-ST-CR encoder groups the N rotated symbols into $N/2$ symbol pairs which are then encoded by the Alamouti encoder [3] and transmitted on $N/2$ antenna pairs in a time-multiplexed fashion. Examples of the such codes are

$$\mathbf{S}(\mathbf{r}) = \begin{cases} \text{diag}(r_1, \cdots, r_N), \text{ ST-CR} \\ \frac{1}{\sqrt{2}}\text{diag}\left(\mathbf{S}_{\text{A}}\left(r_1, r_2\right), \cdots, \mathbf{S}_{\text{A}}\left(r_{N-1}, r_N\right)\right), \text{ A-ST-CR} \end{cases} \tag{3}$$

where $\mathbf{S}_{\text{A}}\left(a, b\right) \triangleq \begin{bmatrix} a & b \\ -b^* & a^* \end{bmatrix}$ denotes the Alamouti codeword [3]. For both codes, the determinants of the $N \times N$ matrices $\mathbf{A} \triangleq \mathbf{S}(\mathbf{r} - \mathbf{r}')^*\mathbf{S}(\mathbf{r} - \mathbf{r}')$ for distinct input vectors $\mathbf{x}$, $\mathbf{x}'$, can be easily calculated as [8]-[10]

$$\det(\mathbf{A}) = \begin{cases} \prod_{i=1}^{N} |d_i|^2, \text{ ST-CR} \\ \prod_{i=1}^{N/2} \frac{1}{4}\left(|d_{2i-1}|^2 + |d_{2i}|^2\right)^2, \text{ A-ST-CR} \end{cases} \tag{4}$$

with $d_i \triangleq r_i - r'_i$ where r_i and r'_i denote the ith entries of $\mathbf{r}$ and $\mathbf{r}'$, respectively. Also, $\mathbf{r}$ and $\mathbf{r}'$ are the precoded vectors corresponding to $\mathbf{x}$ and $\mathbf{x}'$, respectively.

It is noted that the linear precoders $\mathbf{\Theta}$ used in the ST-CR and the A-ST-CR codes [8]-[10] are always designed so that $d_i \neq 0$ (or $r_i \neq r'_i$), $^{\forall}i$, for any two distinct input vectors $\mathbf{x}$, $\mathbf{x}'$, referred to as the *rotation property* [10]. Hence, we can easily observe that the determinants of (4) are always positive due to the rotation property of $\mathbf{\Theta}$ and thus, both the ST-CR and the A-ST-CR codes of (3) satisfy the Tarokh's rank criterion [1], guaranteeing full spatial diversity. Even though these two codes have a same diversity order N, the A-ST-CR code outperforms the ST-CR code due to its improved coding gain [10].

In [7]-[9], the unitary precoders $\mathbf{\Theta}$ optimized in a sense of the Tarokh's determinant criterion [1] were investigated and presented by using algebraic design tools and also an exhaustive search method. Note that unitary (or orthogonal) precoders have a preferable feature of guaranteeing no performance loss in non-fading AWGN channels. This is because unitarity of precoders preserves Euclidean distance between any two constellation points. In particular, the unitary precoders $\mathbf{\Theta}$ based on algebraic design theory are given as [8], [9]

$$\mathbf{\Theta} = \begin{cases} \frac{1}{\sqrt{N}}\text{VDM}(\alpha_0, \alpha_1, \cdots, \alpha_{N-1}), \ N = 2^n \\ \mathbf{F}_N \text{diag}(1, \alpha, \cdots, \alpha^{N-1}), \ N \neq 2^n \end{cases} \tag{5}$$

where VDM and $\mathbf{F}_N$ denote the Vandermonde and the N-point inverse FFT matrices, respectively. Also, $\alpha_i = \exp(j2\pi(i + 1/4)/N)$, $i = 0, \cdots, N-1$ and $\alpha = \exp(j2\pi/P)$ where P is a positive integer. For the specific case of $N = 3$, an optimal $\mathbf{\Theta}$ different from (5) is presented in [8], [9]

$$\mathbf{\Theta} = \begin{bmatrix} 0.687 & 0.513 - 0.113j & -0.428 + 0.264j \\ -0.358 - 0.308j & 0.696 - 0.172j & -0.011 - 0.513j \\ 0.190 + 0.520j & 0.243 - 0.389j & 0.696 \end{bmatrix}. \tag{6}$$

4 Design of New Concatenated STBCs

In Section III, we briefly review the characteristics of the conventional A-ST-CR code in (3) designed by serially concatenated the linear precoders with the Alamouti scheme for even N transmit antennas. In this Section, based on the design structure of this A-ST-CR code, we will present new several concatenated STBCs which can be used in systems with odd $N - 1$ transmit antennas.

4.1 New STBCs Using $\mathbf{\Theta}$ of $N \times N$

One of conventional methods for a STBC with N transmit antennas to be used in systems with $N - 1$ transmit antennas is simply to delete one of column vectors

of the code [2]. Thus, by simply deleting the last column vector of the A-ST-CR code in (3), we may easily construct a new STBC for $N-1$ transmit antennas given as

$$\mathbf{S}(\mathbf{r}) = \sqrt{\frac{N}{2(N-1)}} \begin{bmatrix} \mathbf{S}_{\mathrm{A}}(r_1, r_2) & \cdots & \mathbf{0}_2 & \mathbf{0}_{2\times 1} \\ \vdots & \ddots & \vdots & \vdots \\ \mathbf{0}_2 & \cdots & \mathbf{S}_{\mathrm{A}}(r_{N-3}, r_{N-2}) & \mathbf{0}_{2\times 1} \\ \mathbf{0}_{2\times 1}^T & \cdots & \mathbf{0}_{2\times 1}^T & r_{N-1} \\ \mathbf{0}_{2\times 1}^T & \cdots & \mathbf{0}_{2\times 1}^T & -r_N^* \end{bmatrix} \tag{7}$$

where $\mathbf{0}_2$ and $\mathbf{0}_{2\times 1}$ denote a zero matrix of size 2×2 and a zero column vector of length two, respectively. Also, $\sqrt{N/(2(N-1))}$ is a normalizing factor with the total transmitted power constraint $E\{\|\mathbf{S}(\mathbf{r})\|^2\} = N$. For this code, the determinant of $\mathbf{A}$ matrix of size $(N-1)\times(N-1)$ for any two distinct input vectors $\mathbf{x}$, $\mathbf{x}'$ is computed as

$$\det(\mathbf{A}) = \left(\frac{N}{2(N-1)}\right)^{N-1} \left(\prod_{i=1}^{\frac{N}{2}-1} \left(|d_{2i-1}|^2 + |d_{2i}|^2\right)^2\right) \left(|d_{N-1}|^2 + |d_N|^2\right) \tag{8}$$

where $d_i = r_i - r_i^{'}$ is defined in (4). Hence, due to the rotation property of $\mathbf{\Theta}$, i.e., $d_i \neq 0$, $^{\forall}i$, we can easily know that the determinant of (8) is always positive and thus, the code of (7) achieves full spatial diversity like the conventional ST-CR and A-ST-CR codes. The new code is also full rate because N modulated symbols are transmitted for N symbol time epochs.

It is noted that even though both the A-ST-CR and ST-CR codes achieve same diversity order N with a given $\mathbf{\Theta}$, the A-ST-CR code enjoys larger coding gain than the ST-CR code [10]. This is mainly due to the fact that the A-ST-CR code can transmit the precoded symbols r_i through the Alamouti encoder more reliably than the ST-CR code. From a this point of view, the new code of (7) has still room for increasing coding gain because the last precoded symbol pair (r_{N-1}, r_N) is transmitted on only an $(N-1)$th transmit antenna, not through the Alamouti encoder. Hence, by intuition, we may design a new code different from (7) where the second column vector of $\mathbf{S}_{\mathrm{A}}(r_{N-1}, r_N)$ is transmitted on the $(N-2)$th antenna as follow:

$$\mathbf{S}(\mathbf{r}) = \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbf{S}_{\mathrm{A}}(r_1, r_2) & \cdots & \mathbf{0}_{2\times 1} & \mathbf{0}_{2\times 1} & \mathbf{0}_{2\times 1} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ \mathbf{0}_{2\times 1}^T & \cdots & r_{N-3} & r_{N-2} & 0 \\ \mathbf{0}_{2\times 1}^T & \cdots & -r_{N-2}^* & r_{N-3}^* & 0 \\ \mathbf{0}_{2\times 1}^T & \cdots & 0 & r_N & r_{N-1} \\ \mathbf{0}_{2\times 1}^T & \cdots & 0 & r_{N-1}^* & -r_N^* \end{bmatrix} \tag{9}$$

where $1/\sqrt{2}$ is a normalizing factor with the power constraint of $E\{\|\mathbf{S}(\mathbf{r})\|^2\} = N$. For example, when using three transmit antennas, the code of (9) is given as

$$\mathbf{S}(\mathbf{r}) = \frac{1}{\sqrt{2}} \begin{bmatrix} r_1 & r_2 & 0 \\ -r_2^* & r_1^* & 0 \\ 0 & r_4 & r_3 \\ 0 & r_3^* & -r_4^* \end{bmatrix}. \tag{10}$$

Clearly, the code of (9) is full rate because $T_0 = L$ to be N. This code is also guaranteed to achieve full spatial diversity like the new code of (7) because for any two distinct input vectors $\mathbf{x}$, $\mathbf{x}'$,

$$\det(\mathbf{A}) = \left(\frac{1}{2}\right)^{N-1} \left(\prod_{i=1}^{\frac{N}{2}-2} \left(|d_{2i-1}|^2 + |d_{2i}|^2 \right)^2 \right) \left(|d_{N-3}|^2 + |d_{N-2}|^2 \right) \times \left(|d_{N-3}|^2 + |d_{N-2}|^2 + |d_{N-1}|^2 + |d_N|^2 \right) \left(|d_{N-1}|^2 + |d_N|^2 \right) > 0. \tag{11}$$

Even though both the proposed codes of (7) and (9) achieve full spatial diversity $N-1$ with a given $\mathbf{\Theta}$, the code of (9) outperforms the one of (7) for all SNR values, which will be shown by computer simulations in Section IV.

4.2 New STBC Using $\mathbf{\Theta}$ of $N/2 \times N/2$

As commented in the previous subsection, both the new codes of (7) and (9) using $\mathbf{\Theta}$ of size $N \times N$ have some advantages of achieving full rate and full diversity for general QAM. However, these codes have a great drawback of not satisfying the Tarokh's orthogonal designs [2], leading to a much higher increase in ML decoding complexity at the receiver than the O-STBCs. Hence, in this subsection, by using a linear precoder $\mathbf{\Theta}$ of size $N/2 \times N/2$, a new full rate and full diversity STBC possessing quasi-orthogonal property will be presented for any odd $N-1$ transmit antennas.

The proposed encoder first divides an input vector $\mathbf{x}$ of length N into two input sub-vectors $\mathbf{x}_i = [x_{i,1}, \cdots, x_{i,N/2}]^T$, $i = 1, 2$ of length $N/2$, i.e., $\mathbf{x} = [\mathbf{x}_1, \mathbf{x}_2]^T$. Each of these sub-vectors, $\mathbf{x}_i$ is then multiplied separately by a same linear precoder $\mathbf{\Theta}$ of size $N/2 \times N/2$, resulting in two precoded sub-vectors of length $N/2$, $\mathbf{r}_i = [r_{i,1}, \cdots, r_{i,N/2}]^T = \mathbf{\Theta}\mathbf{x}_i$, $i = 1, 2$. Then, by serially grouping the ith elements in both $\mathbf{r}_1$ and $\mathbf{r}_2$, total $N/2$ precoded symbol pairs $(r_{1,i}, r_{2,i})$, $i = 1, \cdots, N/2$ are generated. These pairs $(r_{1,i}, r_{2,i})$ are then encoded independently by the Alamouti encoder [3] and transmitted on $N-1$ transmit antennas like the new code of (9)

$$\mathbf{S}(\mathbf{r}) = \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbf{S}_{\mathrm{A}}(r_{1,1}, r_{2,1}) & \cdots & \mathbf{0}_{2\times 1} & \mathbf{0}_{2\times 1} & \mathbf{0}_{2\times 1} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ \mathbf{0}_{2\times 1}^T & \cdots & r_{1,\frac{N}{2}-1} & r_{2,\frac{N}{2}-1} & 0 \\ \mathbf{0}_{2\times 1}^T & \cdots & -r_{2,\frac{N}{2}-1}^* & r_{1,\frac{N}{2}-1}^* & 0 \\ \mathbf{0}_{2\times 1}^T & \cdots & 0 & r_{2,\frac{N}{2}} & r_{1,\frac{N}{2}} \\ \mathbf{0}_{2\times 1}^T & \cdots & 0 & r_{1,\frac{N}{2}}^* & -r_{2,\frac{N}{2}}^* \end{bmatrix}. \tag{12}$$

It is clear that this code is full-rate because $T_0 = L$ to be N as the code of (9). For the code of (12), we can easily calculate the determinant of the $\mathbf{A}$ matrix for any distinct input vectors $\mathbf{x}$, $\mathbf{x}'$ as

$$\det(\mathbf{A}) = \left(\frac{1}{2}\right)^{N-1} \left(\prod_{i=1}^{\frac{N}{2}-2} \left(|d_{1,i}|^2 + |d_{2,i}|^2\right)^2\right) \left(\left|d_{1,\frac{N}{2}-1}\right|^2 + \left|d_{2,\frac{N}{2}-1}\right|^2\right) \times \left(\left|d_{1,\frac{N}{2}-1}\right|^2 + \left|d_{2,\frac{N}{2}-1}\right|^2 + \left|d_{1,\frac{N}{2}}\right|^2 + \left|d_{2,\frac{N}{2}}\right|^2\right) \left(\left|d_{1,\frac{N}{2}}\right|^2 + \left|d_{2,\frac{N}{2}}\right|^2\right) \quad (13)$$

with $d_{i,j} = r_{i,j} - r'_{i,j}$ where $r_{i,j}$ and $r'_{i,j}$ represent the jth elements of $\mathbf{r}_i$ and $\mathbf{r}'_i$, respectively.

Indeed, for any two distinct vectors $\mathbf{x}$, $\mathbf{x}'$, there exists at least one sub-vector pair $(\mathbf{x}_i, \mathbf{x}'_i)$ satisfying $\mathbf{x}_i \neq \mathbf{x}'_i$. This implies $r_{i,j} \neq r'_{i,j}$ (or $d_{i,j} \neq 0$), $^\forall j$, for a given index i because of the rotation property of $\mathbf{\Theta}$. Hence, the determinant of (13) is always positive and thus, the code of (12) enjoys full spatial diversity of order $N-1$ like the new codes of (7) and (9). This code also satisfies the quasi-orthogonal property like the conventional quasi-orthogonal STBCs (QO-STBCs) [4]-[6], allowing a ML decoder at the receiver to decode the two sub-vectors $\mathbf{x}_1$, $\mathbf{x}_2$, independently, which will be derived in the following.

First, by complex-conjugating the all elements of even indices in $\mathbf{y}$, denoted as $\mathbf{y}'$, we can easily rearrange the ML metric given in (2) for the code of (12) as follow:

$$\|\mathbf{y} - \mathbf{S}(\mathbf{x})\mathbf{h}\| = \left\|\mathbf{y}' - \mathbf{H} \begin{bmatrix} \mathbf{\Theta} & \mathbf{0}_{\frac{N}{2}} \\ \mathbf{0}_{\frac{N}{2}} & \mathbf{\Theta} \end{bmatrix} \mathbf{x}\right\| \quad (14)$$

with

$$\mathbf{H} \triangleq \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbf{h}_{1,\frac{N}{2}+1}(h_1, h_2) \\ \vdots \\ \mathbf{h}_{\frac{N}{2}-1,N-1}(h_{N-3}, h_{N-2}) \\ \mathbf{h}_{\frac{N}{2},N}(h_{N-1}, h_{N-2}) \end{bmatrix} \quad (15)$$

where $\mathbf{h}_{i,j}(a,b)$ denotes an $2 \times N$ matrix whose ith and jth column vectors are $[a, b^*]^T$ and $[b, -a^*]^T$, respectively, and all other column vectors with zero elements. The equality of (14) uses the fact that the conjugating of any number of elements in a vector preserves the magnitude of the vector. At this point of time, we will define an unitary matrix $\mathbf{B}$ generated by appropriately normalizing the elements in $\mathbf{H}$ of (15), given as

$$\mathbf{B} \triangleq \begin{bmatrix} \mathbf{h}_{1,\frac{N}{2}+1}(h_1, h_2)/\rho(h_1, h_2) \\ \vdots \\ \mathbf{h}_{\frac{N}{2}-1,N-1}(h_{N-3}, h_{N-2})/\rho(h_{N-3}, h_{N-2}) \\ \mathbf{h}_{\frac{N}{2},N}(h_{N-1}, h_{N-2})/\rho(h_{N-1}, h_{N-2}) \end{bmatrix} \quad (16)$$

where $\rho(a,b) \triangleq \sqrt{|a|^2+|b|^2}$. Note that the matrix $\mathbf{B}$ of (16) satisfies the unitarity, i.e., $\mathbf{B}^*\mathbf{B} = \mathbf{I}_N$ where $\mathbf{I}_N$ represents an identity matrix of size $N \times N$.

Then by using the complex conjugate of $\mathbf{B}$ of (16), the ML metric in the right side of (14) can be decomposed into two functions composed of $\mathbf{x}_1$ and $\mathbf{x}_2$, respectively, as follows:

$$\left\|\mathbf{y}' - \mathbf{H}\begin{bmatrix} \mathbf{\Theta} & \mathbf{0}_{\frac{N}{2}} \\ \mathbf{0}_{\frac{N}{2}} & \mathbf{\Theta} \end{bmatrix}\mathbf{x}\right\| = \left\|\mathbf{B}^*\mathbf{y}' - \mathbf{B}^*\mathbf{H}\begin{bmatrix} \mathbf{\Theta} & \mathbf{0}_{\frac{N}{2}} \\ \mathbf{0}_{\frac{N}{2}} & \mathbf{\Theta} \end{bmatrix}\mathbf{x}\right\| \tag{17}$$

$$= \left\|\begin{bmatrix} \mathbf{z}_1 \\ \mathbf{z}_2 \end{bmatrix} - \begin{bmatrix} \mathbf{\Lambda} & \mathbf{0}_{\frac{N}{2}} \\ \mathbf{0}_{\frac{N}{2}} & \mathbf{\Lambda} \end{bmatrix}\begin{bmatrix} \mathbf{\Theta} & \mathbf{0}_{\frac{N}{2}} \\ \mathbf{0}_{\frac{N}{2}} & \mathbf{\Theta} \end{bmatrix}\begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix}\right\| \tag{18}$$

$$= \sum_{i=1}^{2} \|\mathbf{z}_i - \mathbf{\Lambda\Theta}\mathbf{x}_i\| \tag{19}$$

where $[\mathbf{z}_1, \mathbf{z}_2]^T = \mathbf{B}^*\mathbf{y}'$ with $N/2$ dimensional vectors $\mathbf{z}_1$, $\mathbf{z}_2$ and

$$\mathbf{\Lambda} \triangleq \frac{1}{\sqrt{2}}\mathrm{diag}\left(\rho\left(h_1, h_2\right), \cdots, \rho\left(h_{N-3}, h_{N-2}\right), \rho\left(h_{N-1}, h_{N-2}\right)\right).$$

The equality of (17) uses the unitarity of the matrix $\mathbf{B}$ preserving the energy of a vector. Hence, we can easily know that the minimization of the ML metric in the left of (17) is equivalent to the minimization of the two equations of $\mathbf{x}_1$ and $\mathbf{x}_2$ in (19), separately. Thus, the ML receiver for the code of (12) can decode the input sub-vectors $\mathbf{x}_i$, independently, by choosing $\hat{\mathbf{x}}_i$ such that

$$\hat{\mathbf{x}}_i = arg\min_{\mathbf{x}_i} \|\mathbf{z}_i - \mathbf{\Lambda\Theta}\mathbf{x}_i\|, \quad i = 1, 2. \tag{20}$$

5 Simulation Results

All of STBCs considered in this Section are assumed to be ones with N_t transmit and one receive antennas over quasi-static Rayleigh fading channels. Also, it is assumed that the fading channel gains are perfectly known at the receiver. With these assumptions, we provide the simulation results of the three proposed codes of (7), (9) and (12) with $N_t = 3, 5$ for QPSK and $N_t = 3$ for 16-QAM. The codes of (7) and (9) use the same unitary precoders $\mathbf{\Theta}$ of (5) of size 4×4 for $N_t = 3$ and of size 6×6 with $P = 36$ for $N_t = 5$, respectively. Also, the quasi-orthogonal code of (12) uses $\mathbf{\Theta}$ of size 2×2 constructed using (5) for $N_t = 3$ and $\mathbf{\Theta}$ given in (6) for $N_t = 5$. For the comparison of performances, the results of the ST-CR code [9], [10] in (3) using $\mathbf{\Theta}$ of (5) and the Alamouti scheme [3] are also included. Furthermore, we include the results of the maximal ratio receiver combining (MRRC) scheme using appropriately normalized one transmit and N_t receive antennas [3].

Figs. 2 and 3 show the average symbol error rate (SER) curves versus E_s/N_0 for QPSK and 16-QAM, respectively. From these results, we see that all of the

proposed codes achieve full spatial diversity and also, larger coding gains than the existing ST-CR code [8], [9] for all SNR values. This is because the proposed codes can transmit the precoded symbols r_i more reliably than the conventional ST-CR code by using the Alamouti encoder with two transmit antennas. In particular, the code of (9) is shown to achieve the best performance among the three proposed codes for all considered modulations and transmit antennas. For the case of QPSK, this code enjoys approximately 1.5dB larger coding gain than the existing ST-CR code for $N_t = 3, 5$ at average SER=10^{-5} and for the case of 16-QAM, 3dB for $N_t = 3$. Also, we notice that the best code exhibits error performance within only about 1dB of the MRRC scheme.

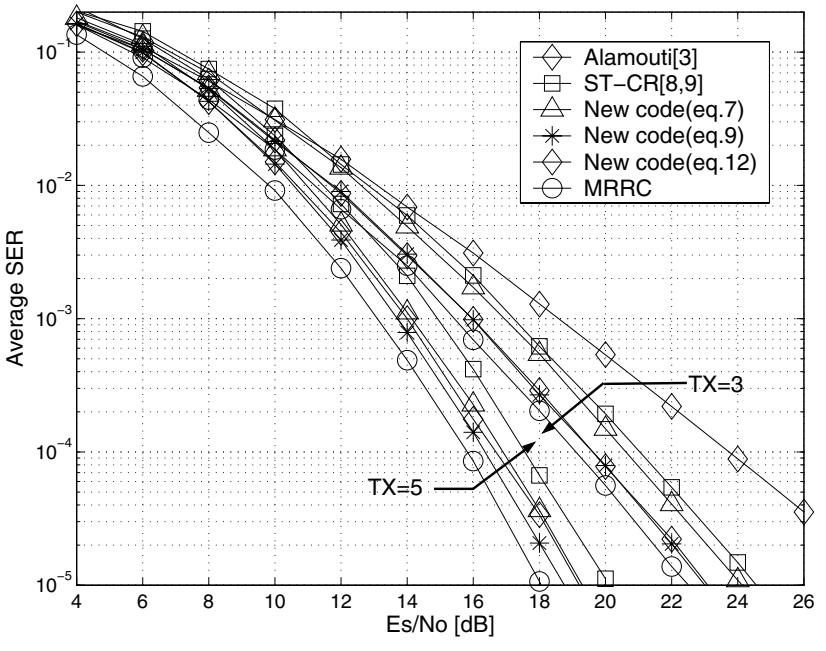


Fig. 2. Average SER versus E_s/N_0 [dB] for QPSK

We also know from these results that the proposed quasi-orthogonal code of (12) exhibits approximately same error performance as the best code of (9) for all SNR values for considered modulations and transmit antennas. It is noted that this code satisfies the quasi-orthogonal characteristic like the conventional QO-STBCs [4]-[6], leading to greatly simplified ML decoding at the receiver. Hence, considering both the performance results and the decoding complexity, this code may be a promising solution for the next generation mobile communications.

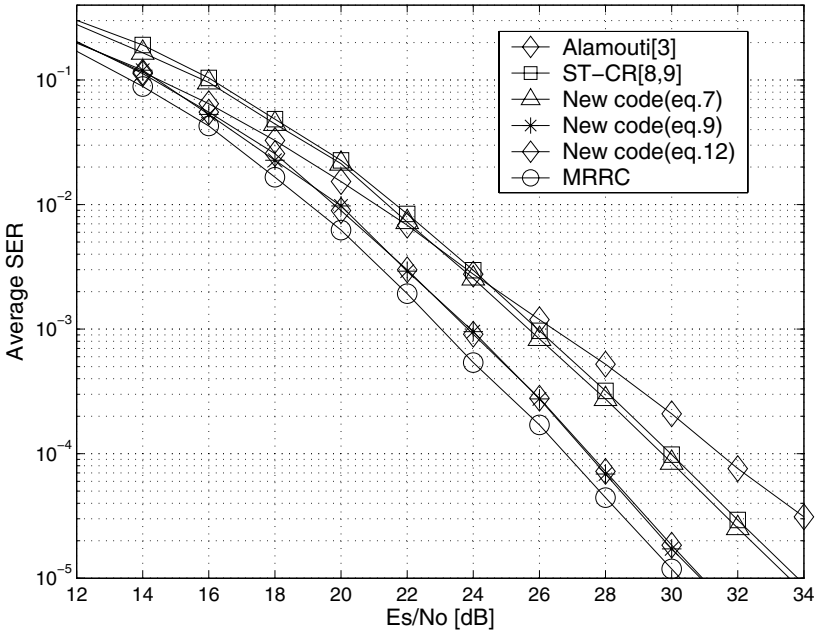


Fig. 3. Average SER versus E_s/N_0 [dB] for 16-QAM and three transmit antennas

6 Conclusions

In this paper, we proposed new STBCs achieving full rate and full diversity for QAM and quasi-static Rayleigh fading channels when using any odd number of transmit antennas. These codes are designed by serially concatenating the constellation-rotating precoders with the Alamouti scheme like the conventional A-ST-CR code. We showed by computer simulations that all of proposed codes outperform the existing ST-CR codes for any considered modulations and transmit antennas. Particularly, the codes possessing quasi-orthogonal characteristic are also included in this class, allowing simple ML decoding with virtually no performance loss compared to the best code in the class.

References

1. V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, no. 2, pp. 744-765, Mar. 1998.
2. V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block coding for wireless communications: Theory of generalized orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1456-1467, July 1999.

3. S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Select. Areas Commun.*, vol. 16, no. 8, pp. 1451-1458, Oct. 1998.
4. H. Jafarkhani, "A quasi-orthogonal space-time block code," *IEEE Trans. Commun.*, vol. 49, pp. 1-4, Jan. 2001.
5. N. Sharma and C. B. Papadias, "Improved quasi-orthogonal codes through constellation rotation," *IEEE Trans. Commun.*, vol. 52, pp. 332-335, Mar. 2003.
6. W. Su and X.-G. Xia, "Signal constellations for quasi-orthogonal space-time block codes with full diversity," *IEEE Trans. Inform. Theory*, vol. 50, pp. 2331-2347, Oct. 2004.
7. X. Giraud and E. Boutillon, and J. C. Belfore, "Algebraic tools to build modulation schemes for fading channels," In *IEEE Trans. Inform. Theory*, vol. 43, pp. 938-952, May 1997.
8. Y. Xin, Z. Wang, and G. B. Giannakis, "Space-time constellation-rotating codes maximizing diversity and coding gains," in *Proc. GLOBECOM*, vol. 1, pp. 455-459, 2001.
9. Y. Xin, Z. Wang, and G. B. Giannakis, "Space-time diversity systems based on linear constellation precoding," *IEEE Tran. Wireless Commun.* vol. 2, pp. 294-309, Mar. 2003.
10. T. Jung and K. Cheun, "Design of concatenated space-time block codes using signal space diversity and the Alamouti scheme," *IEEE Commun. Lett.*, vol. 7, pp. 329-331, July 2003.

Performance of Downlink Group-Orthogonal Multicarrier Systems

Felip Riera-Palou, Guillem Femenias, and Jaume Ramis

Dept. of Mathematics and Informatics
University of the Balearic Islands
07122 Palma de Mallorca, Spain
{felip.riera, guillem.femenias, jaume.ramis}@uib.es

Abstract. Group-orthogonal multi-carrier code division multiple access (GO-MC-CDMA) has recently been proposed as a promising technique for the uplink segment of wireless systems. In this paper we propose and analyze a related scheme, group-orthogonal multi-carrier code division multiplexing (GO-MC-CDM), suitable for the downlink segment. The proposed receiver is shown to offer a similar bit error rate (BER) performance as the downlink version of GO-MC-CDMA at a fraction of its computational complexity. An analytical expression for the BER when using maximum likelihood (ML) detection is derived providing valuable insight into the parameters affecting the system performance and providing a basis for its optimization. Simulation results using parameters and channel models aiming at the next generation of wireless systems are provided confirming the analytically derived results.

Keywords: MC-CDMA, downlink, multi-symbol detection, rotated spreading.

1 Introduction

Multi-carrier code division multiple access (MC-CDMA) [1] can be seen as a specific case (see [2] for other possibilities) of the combination of two complementary techniques: code division multiple access (CDMA) and orthogonal frequency division multiplexing (OFDM). On one hand, CDMA multiplexes users by means of a user-specific spreading code allowing them to simultaneously use the same frequency spectrum. The properties of these codes (e.g. orthogonality) make user separation at the receiver possible. On the other hand, OFDM is a block transmission scheme where the incoming user symbols are grouped, serial-to-parallel (S/P) converted and modulated onto different subcarriers. Choosing the subcarriers to be orthogonal allows the group of symbols to be transmitted in parallel without interference. The S/P conversion permits the transmission rate to be reduced to a fraction of the original user rate combating in this way the frequency selectivity of the channel. The attractive features derived from the CDMA-OFDM combination makes MC-CDMA a firm candidate for the next generation of wireless systems [3]. Typically, multiuser detection (MUD) based on linear or non-linear processing is employed in the uplink due to its superior

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 389–400, 2006.

performance and the lack of tight computational constraints in the base stations [3]. In the downlink, single-user detection is usually preferred owing to its lower computational cost.

Group-orthogonal MC-CDMA (GO-MC-CDMA) has been recently proposed in [4] as an attractive alternative for the uplink segment. It can be seen as the combination of MC-CDMA and orthogonal frequency division multiple access (OFDMA). The main idea behind GO-MC-CDMA is to partition the available (orthogonal) subcarriers into (orthogonal) groups and distribute users among the groups. The main advantage of this system is that each group functions as an independent MC-CDMA system with a smaller number of users making the use of maximum likelihood multiuser detection (ML-MUD) within each group feasible.

As with MC-CDMA, GO-MC-CDMA can in principle also be used for the downlink. The mobile user can then employ a detector targeting only the subcarriers forming the groups where his symbols are being transmitted. Notice that in the usual case where several symbols in parallel are transmitted for each user, the receiver will need a separate detector for each required group. As in the uplink, and depending on the resources available at the receiver, each group-wise detector can be single-user or multiuser [3]. This latter case can be considered as rather inefficient since all the detected symbols in a group but one will be discarded as they belong to other active users in the network. A more appropriate solution consists of multiplexing all the (parallel) symbols from a given user in the same group similar to the OFDM code-division multiplexing (OFDM-CDM) scheme proposed in [5] hence the name of our proposal, group-orthogonal multicarrier code-division multiplexing (GO-MC-CDM). In contrast with (downlink) GO-MC-CDMA, in the proposed system the mobile user needs only targeting one single group which contains all the useful information, making multisymbol (rather than single symbol) detection more adequate as it can achieve the same performance as the multiuser counterpart (i.e. GO-MC-CDMA) at a fraction of its complexity.

In this paper we first present the architecture of the GO-MC-CDM and derive an analytical expression for the BER when employing maximum likelihood multisymbol detection (ML-MSD). Relevant parameters affecting the performance are identified allowing some design decisions to be optimally made. Simulation results are then provided, using typical parameters currently under discussion for the next generation of wireless systems, which illustrate the performance of GO-MC-CDM and serve also to validate the analytical results. We note that the analysis presented in this paper would also be valid for the downlink GO-MC-CDMA, although as pointed out before, if multiple symbols are transmitted in parallel, then a separate ML detector would be required for each group.

2 System Model for GO-MC-CDM

This paper focuses on the (synchronous) downlink (base to mobile) of a multicarrier system with N_{total} subcarriers serving K_{total} users. Similarly to

GO-MC-CDMA, the total number of subcarriers is partitioned into $N_g{=}N_{total}/N$ groups where N is the number of subcarriers per group. Each active user in the system has exclusive use of the subcarriers forming a group. Due to the orthogonality among groups, multiuser interference is completely eliminated and therefore only self interference (i.e. inter symbol) should be addressed. Notice that N is the parameter balancing the capacity of the system (number of users) and the maximum number of parallel symbols each user can transmit. Since groups are independent of each other, all the modeling and analysis can be performed on a single group which, to all effects, resembles the OFDM-CDM system proposed in [5].

The block diagram for the base station transmitter corresponding to user k is shown in Fig. 1. At (discrete) time instant n, a block of S successive data symbols $\mathbf{a}^k(n) = [a_0^k \ a_1^k \dots a_{S-1}^k]^T$ with each symbol drawn from an M-ary complex-valued symbol constellation (e.g., M-QAM or M-PSK) and satisfying $E[|a_s^k|^2] = 1$, is first serial-to-parallel converted. Each symbol a_p^k is then multiplied by a different spreading code of the form $\mathbf{c}^s = [c_0^s \ c_1^s \dots c_{N-1}^s]^T$ with $E[|c_i^s|^2] = 1/N$. For later convenience, we define now the $N \times P$ spreading matrix as $\mathbf{C} = [\mathbf{c}^0 \ \mathbf{c}^1 \dots \mathbf{c}^{S-1}]$. The resulting spread symbols are added up and modulated, typically using the inverse fast Fourier transform (IFFT), onto the set of N orthogonal subcarriers forming the group assigned to user k. A cyclic prefix (CP) is appended to the resulting signal to minimise the effects of the channel dispersion. Assuming that the CP length exceeds the maximum channel delay spread, there will not be interference among successively transmitted blocks of symbols.

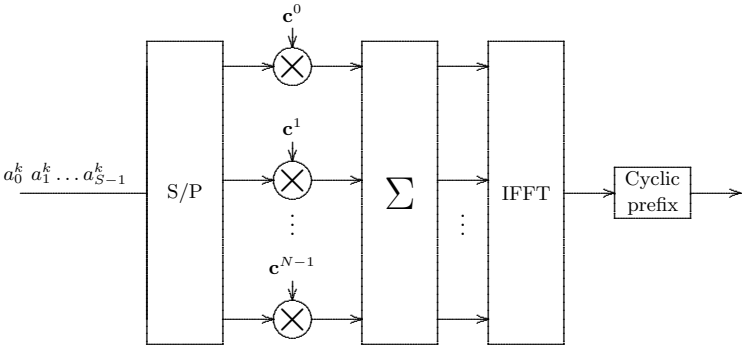


Fig. 1. GO-MC-CDM (group) transmitter

The signal from the base station reaches mobile user k by propagating through a frequency selective channel with an scenario-dependent power delay profile $\mathcal{P}(\tau)$ given by

$$\mathcal{P}(\tau) = \sum_{l=0}^{P-1} \phi(l)\delta(\tau - \tau_l) \tag{1}$$

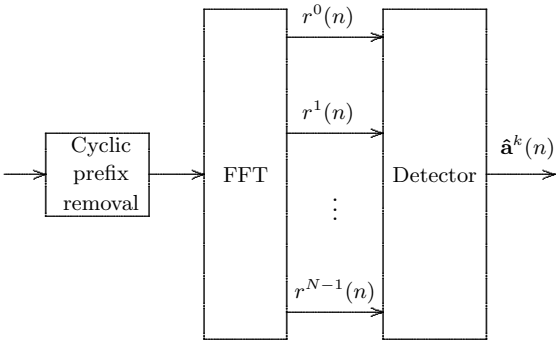


Fig. 2. GO-MC-CDM receiver

where P denotes the number of independent paths of the channel and $\phi(l)$ and τ_l denote the power and delay of each path. It is assumed that the power delay profile is normalized to unity (i.e. $\sum_{l=1}^{l=P} \phi(l) = 1$). A single realization of the channel impulse response from the base station to mobile user k at time instant t will then have the form

$$h^k(t;\tau) = \sum_{l=0}^{P-1} h_l^k(t)\delta(t-\tau_l) \tag{2}$$

where it will hold that $E\left[\mid h_l^k(t) \mid^2\right] = \phi(l)$. The corresponding frequency response will be given by

$$\bar{h}^k(t;f) = \sum_{l=0}^{P-1} h_l^k(t)\exp(-j2\pi f\tau_l) \tag{3}$$

which when evaluated at the N subcarrier frequencies assigned to user k, yields the $N \times 1$ vector $\bar{\mathbf{h}}^k(t) = [\bar{h}^k(t;f_0)\ \bar{h}^k(t;f_1)\ldots\bar{h}^k(t;f_{N-1})]$. Assuming that the channel is static over the duration of a block of S symbols and to simplify the notation, we will express the subcarrier frequency response for user k during the discrete time instant n as $\bar{\mathbf{h}}^k(n) = [\bar{h}_0^k(n)\ \bar{h}_1^k(n)\ldots\bar{h}_{N-1}^k(n)]$.

The reception process at the mobile receiver is illustrated in Fig. 2. After removing the cyclic prefix and assuming perfect subcarrier synchronization, the received signal is sampled and demodulated (tipically using the FFT) yielding the $N \times 1$ received signal vector which can be expressed as

$$\mathbf{r}(n) = \mathbf{H}(n)\mathbf{C}\ \mathbf{a}^k(n) + \mathbf{v}(n) \tag{4}$$

where $\mathbf{H}(n) = \mathcal{D}(\bar{\mathbf{h}}^k(n))$ with $\mathcal{D}(\mathbf{x})$ denoting the squared diagonal matrix having vector $\mathbf{x}$ at its main diagonal. The $N \times S$ system matrix $\mathbf{A}(n)$ is defined as $\mathbf{A}(n) = \mathbf{H}(n)\mathbf{C}$ and represents the combination of channel and spreading effects.

It can easily be seen that $\mathbf{A}(n)$ has the following structure

$$\mathbf{A}(n) = \begin{pmatrix} \bar{h}_0^k(n)c_0^0 & \dots & \bar{h}_0^k(n)c_0^{S-1} \\ \bar{h}_1^k(n)c_1^0 & \dots & \bar{h}_1^k(n)c_1^{S-1} \\ \vdots & \ddots & \vdots \\ \bar{h}_{N-1}^k(n)c_{N-1}^0 & \dots & \bar{h}_{N-1}^k(n)c_{N-1}^{S-1} \end{pmatrix}. \tag{5}$$

The $N \times 1$ complex vector $\mathbf{v}(n)$ is made of zero-mean complex Gaussian random variables with variance $E[v(n)^2] = \sigma_v^2$. Notice that with the definition of normalized unit-power transmitted symbols and normalized power delay profile, the operating signal-to-noise ratio can be expressed as $E_s/N_0 = 1/\sigma_v^2$. In order to simplify the notation, and since successive symbols are independent from one another due to the CP, the explicit time relation will be dropped from subsequent equations. Likewise and since the analysis focuses only on one group (i.e. user), the user index k will also be dropped from now on.

At the mobile receiver, when using maximum likelihood multi-symbol detection (ML-MSD), the symbol estimates are computed according to [6]

$$\hat{\mathbf{a}} = \underset{\mathbf{a}}{\operatorname{argmin}} \|\mathbf{A}\mathbf{a} - \mathbf{r}\|^2. \tag{6}$$

This procedure usually implies evaluating all the possible transmitted blocks of symbols and choosing the closest one (in a least-squares sense) to the received block. Recently, sphere detection [7] has been proposed for efficiently performing this search.

3 Maximum Likelihood Detection Analysis

The probability of symbol error when S symbols are transmitted in a group can be upper bounded using the union bound as

$$P_s \leq \frac{1}{S} \sum_{i=1}^{M^S} \sum_{j=1, j\neq i}^{M^S} P(\mathbf{a}_i) P(\mathbf{a}_i \to \mathbf{a}_j) \mathcal{N}_s(\mathbf{a}_i, \mathbf{a}_j) \tag{7}$$

where $P(\mathbf{a}_i)$ is the probability of transmitting the $S \times 1$ block vector $\mathbf{a}_i$, $P(\mathbf{a}_i \to \mathbf{a}_j)$ represents the pairwise error probability (PEP) of erroneously detecting the $S \times 1$ block vector $\mathbf{a}_j$ and $\mathcal{N}_s(\mathbf{a}_i, \mathbf{a}_j)$ is the number of differing symbols between $\mathbf{a}_i$ and $\mathbf{a}_j$. Using the fact that all block vectors have the same probability of transmission, the probability of bit error can be upper bounded as

$$P_b \leq \frac{1}{SM^S \log_2 M} \sum_{i=1}^{M^S} \sum_{j=1, j\neq i}^{M^S} P(\mathbf{a}_i \to \mathbf{a}_j) \mathcal{N}_b(\mathbf{a}_i, \mathbf{a}_j). \tag{8}$$

where $\mathcal{N}_b(\mathbf{a}_i, \mathbf{a}_j)$ is the number of differing bits between blocks $\mathbf{a}_i$ and $\mathbf{a}_j$.

To progress further in the analysis, the PEP conditioned on the system matrix $\mathbf{A}$ is first calculated. This can then be averaged with respect to $\mathbf{A}$ to yield the

unconditional PEP. The PEP conditioned on a given system matrix $\mathbf{A}$ can be shown to be [8]

$$\begin{aligned} P\left(\mathbf{a}_i \rightarrow \mathbf{a}_j \,|\, \mathbf{A}\right) =& \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\|\mathbf{A}(\mathbf{a}_i - \mathbf{a}_j)\|^2}{4\sigma_v^2}}\right) \\ =& \frac{1}{\pi}\int_0^{\pi/2} \exp\left(-\frac{\| \mathbf{A}(\mathbf{a}_i - \mathbf{a}_j) \|^2}{4\sigma_v^2 \sin^2\phi}\right) d\phi \end{aligned} \tag{9}$$

We now define the error vector $\mathbf{e}_{ij} = \mathbf{a}_i - \mathbf{a}_j = [e_{ij}^0,\ e_{ij}^1, \ldots,\ e_{ij}^{S-1}]$ and the $N \times N$ diagonal matrix

$$\mathbf{T}_{ij} = \begin{pmatrix} \sum_{s=0}^{S-1} e_{ij}^s c_0^s & 0 & \ldots & 0 \\ 0 & \sum_{s=0}^{S-1} e_{ij}^s c_1^s & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & \sum_{s=0}^{S-1} e_{ij}^s c_{N-1}^s \end{pmatrix} \tag{10}$$

We also define the $N \times N$ channel correlation matrix $\mathbf{R} = E[\bar{\mathbf{h}}\bar{\mathbf{h}}^H]$ which can be determined from the Fourier transform of $\mathcal{P}(\tau)$ (spaced-frequency correlation function) evaluated at the group-assigned subcarrier frequencies. It can be shown that $d_{ij}^2 \triangleq \| \mathbf{A}(\mathbf{a}_i - \mathbf{a}_j) \|^2 = \mathbf{e}_{ij}^H \mathbf{A}^H \mathbf{A} \mathbf{e}_{ij} = \bar{\mathbf{h}}^H \mathbf{T}_{ij}^H \mathbf{T}_{ij}\ \bar{\mathbf{h}}$ is a quadratic form in complex variable $\bar{\mathbf{h}}$ with moment generating function (MGF)[9]

$$M_{d^2,ij}(w) = \left|\mathbf{I} + w\mathbf{T}_{ij}\mathbf{R}\mathbf{T}_{ij}^H\right|^{-1}. \tag{11}$$

Let $\boldsymbol{\lambda}_{ij} = \{\lambda_{ij,1}, \lambda_{ij,2}, \ldots,\ \lambda_{ij,D_{ij}}\}$ denote the set of D_{ij} distinct positive eigenvalues of $\mathbf{K}_{ij} = \mathbf{T}_{ij}\mathbf{R}\mathbf{T}_{ij}^H$ where the multiplicity of each eigenvalue is given by $\alpha_{ij,1}, \alpha_{ij,2}, \ldots,\ \alpha_{ij,D_{ij}}$. It is shown in [10] that the MGF of d_{ij}^2 can also be expressed as

$$M_{d^2,ij}(w) = \prod_{d=1}^{D_{ij}} \frac{1}{(1 + w\lambda_{ij,d})^{\alpha_{ij,d}}} = \sum_{d=1}^{D_{ij}} \sum_{p=1}^{\alpha_{ij,d}} \frac{\kappa_{ij,d,p}}{(1 + w\lambda_{ij,d})^p} \tag{12}$$

where

$$\kappa_{ij,d,p} = \frac{\lambda_{ij,d}^{p-\alpha_{ij,d}}}{(\alpha_{ij,d} - p)!} \frac{\partial^{\alpha_{ij,d}-p}}{\partial^{\alpha_{ij,d}-p} w} \left[\prod_{\substack{d'=1 \\ d' \neq d}}^{D_{ij}} \frac{1}{(1 + w\lambda_{ij,d'})^{\alpha_{ij,d'}}}\right]\Bigg|_{w=-\frac{1}{\lambda_{ij,d}}}$$

which allows the unconditional PEP to be written as

$$\begin{aligned} P\left(\mathbf{a}_i \rightarrow \mathbf{a}_j\right) &= \frac{1}{\pi}\sum_{d=1}^{D_{ij}} \sum_{p=1}^{\alpha_{ij,d}} \kappa_{ij,d,p} \int_0^{\pi/2} \left(\frac{\sin^2\phi}{\sin^2\phi + \frac{\lambda_{ij,d}}{4\sigma_v^2}}\right)^p d\phi \\ &= \sum_{d=1}^{D_{ij}} \sum_{p=1}^{\alpha_{ij,d}} \kappa_{ij,d,p} \left(\frac{1 - \Omega(\frac{\lambda_{ij,d}}{4\sigma_v^2})}{2}\right)^p \sum_{g=0}^{p-1} \binom{p-1+g}{g} \left(\frac{1 + \Omega(\frac{\lambda_{ij,d}}{4\sigma_v^2})}{2}\right)^g \end{aligned} \tag{13}$$

with $\Omega(c) = \sqrt{c/(1+c)}$. By substituting (13) into (8), a closed-form BER upper bound for an arbitrary power delay profile is obtained. It is later shown that this bound is tight and accurately matches the simulation results.

Since there are many pairs $(\mathbf{a}_i, \mathbf{a}_j)$ giving exactly the same PEP, it is possible to define a pairwise error class $\mathcal{C}(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c)$ as the set of all pairs $(\mathbf{a}_i, \mathbf{a}_j)$ characterized with a matrix $\mathbf{K}_{ij}$ with rank $\hat{D}_c$ and a set of eigenvalues $\hat{\boldsymbol{\lambda}}_c = \{\hat{\lambda}_{c,1}, \ldots, \hat{\lambda}_{c,\hat{D}_c}\}$ and therefore, a common PEP denoted by $\mathrm{PEP}(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c)$. A more insightful BER expression (in comparison with (8)) can then be obtained by using the PEP class notation, avoiding the exhaustive computation of all the PEPs. Instead, the BER upper-bound can be found by finding out the PEP for each class and weighing it using the number of elements in the class and the number of erroneous bits this class may induce. The BER upper bound can then be rewritten as

$$P_b \leq \frac{1}{SM^S \log_2 M} \sum_{\forall \mathcal{C}(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c)} \sum_{i=1}^{S log_2 M} W(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c, i)\ i\ \mathrm{PEP}(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c) \tag{14}$$

where $W(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c, i)$ corresponds to the number of elements in the class $\mathcal{C}(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c)$ inducing i erroneous bits.

4 Asymptotic Performance

In order to gain further insight on the parameters affecting the BER in a GO-MC-CDM system, we now focus on the asymptotic case of large E_s/N_0. It is easy to see that when $w \to \infty$ the MGF from (12) can be approximated by

$$M_{d^2,ij}(w) \simeq \frac{1}{\left(\prod_{d=1}^{D_{ij}} \lambda_{ij,d}^{\alpha_{ij,d}}\right) w^{\sum_{d=1}^{D_{ij}} \alpha_{ij,d}}} \tag{15}$$

allowing $\mathrm{PEP}(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c)$ for large E_s/N_0 to be expressed as

$$\begin{aligned} \mathrm{PEP}_{\mathrm{asym}}\left(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c\right) &= \frac{1}{\pi} \int_0^{\pi/2} \frac{(4\sigma_v^2 \sin^2\phi)^{\hat{D}_c}}{\prod_{d=1}^{\hat{D}_c} \hat{\lambda}_{c,d}^{\hat{\alpha}_{c,d}}} d\phi \\ &= \frac{\Gamma\left(\hat{D}_c + \frac{1}{2}\right)}{2\sqrt{\pi}\,\Gamma\left(\hat{D}_c + 1\right)} \frac{\left(4\sigma_v^2\right)^{\hat{D}_c}}{\prod_{d=1}^{\hat{D}_c} \hat{\lambda}_{c,d}^{\hat{\alpha}_{c,d}}} = \frac{(2\hat{D}_c)!}{2\hat{D}_c!^2} \frac{(E_s/N_0)^{-\hat{D}_c}}{\prod_{d=1}^{\hat{D}_c} \hat{\lambda}_{c,d}^{\hat{\alpha}_{c,d}}} \end{aligned} \tag{16}$$

where $\Gamma(x)$ denotes the Gamma function. Equation (16) implies that, asymptotically, the dominant terms in (14) are those corresponding to pairwise error classes associated with $\mathbf{K}$-matrices of minimum rank, that is, $\hat{D}_c = \hat{D}_{min}$, allowing the BER to be asymptotically approximated by

$$P_b \leq \frac{1}{S\ M^S \log_2 M} \sum_{\forall \mathcal{C}(\hat{D}_{min}, \hat{\boldsymbol{\lambda}}_c)} \sum_{i=1}^{S log_2 M} i\ \frac{(2\hat{D}_{min})!}{2(\hat{D}_{min}!)^2} \frac{W(\hat{D}_{min}, \hat{\boldsymbol{\lambda}}_c, i) \left(\frac{E_s}{N_0}\right)^{-\hat{D}_{min}}}{\prod_{d=1}^{\hat{D}_{min}} \hat{\lambda}_{c,d}^{\hat{\alpha}_{c,d}}} \tag{17}$$

This expression indicates that BER can be minimized by simultaneously maximizing $\hat{D}_{min}$ and $\prod_{d=1}^{\hat{D}_{min}} \hat{\lambda}_{c,d}^{\hat{\alpha}_{c,d}}$, therefore it is important to carefully perform the subcarrier allocation and the selection of the family of spreading codes with these objectives in mind. As it happens in the uplink [4], choosing the subcarriers for a group equispaced across the whole bandwidth minimizes subcarrier correlation allowing us to optimize the system performance if an adequate family of codes is properly selected. To this end, rotated spreading transforms have been proposed for downlink multicarrier systems [11].

5 Rotated Spreading

It is shown in [11] that the often used Walsh-Hadamard codes lead to poor diversity gains when employed to perform the frequency spreading in the downlink of multicarrier systems. This can be explained by the fact that for certain symbol blocks, the energy is concentrated on one single subcarrier. A deep fade on this subcarrier dramatically raises the probability of error in the detection process, irrespective of the state of all other subcarriers, limiting in this way the achievable diversity order (asymptotic BER slope) to one. A similar effect is observed in the GO-MC-CDM framework under study which is best illustrated through an example: suppose 4 subcarriers are used to transmit 4 symbols multiplexed by code using binary modulation with alphabet $\{+1, -1\}$ and Walsh-Hadamard spreading. In order to find the BER upper-bound, the different pairwise error classes need to be computed as indicated by (14). One of these classes will comprise the PEP between blocks which differ in all symbols such as $a_i = [1\ 1\ 1\ 1]^T$ and $a_j = [-1\ -1\ -1\ -1]^T$. In this situation it can easily be seen that,

$$\mathbf{T}_{i,j} = \begin{pmatrix} 8\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \end{pmatrix}, \qquad \mathbf{K}_{i,j} = \begin{pmatrix} 8R_{0,0}\,0\,0\,0 \\ 8R_{1,0}\,0\,0\,0 \\ 8R_{2,0}\,0\,0\,0 \\ 8R_{3,0}\,0\,0\,0 \end{pmatrix} \tag{18}$$

where $R_{x,y}$ denotes the (x, y)th entry of the channel correlation matrix. Obviously, for this particular PEP, $\hat{D}_{min} = 1$ and this will become the dominant term in the BER expression given by (14) leading to a diversity order of one. For the particular case of Walsh-Hadamard sequences, this behavior is due to the fact that all columns (or rows) add up to zero except for the first entry. A similar effect can be observed in other spreading sequences such as those based on the discrete Fourier transform (DFT). As pointed out in [11], a spreading that maximizes the diversity gain can be found by applying a rotation to the columns of the conventional spreading matrix $\mathbf{C}$

$$\mathbf{C}_{\text{rot}} = \mathbf{C}\mathcal{D}(\boldsymbol{\theta}) \tag{19}$$

where $\boldsymbol{\theta} = [\theta_0\ \theta_1 \ldots \theta_{N-1}]$ with each θ_i denoting the chip-specific rotation which in the scheme proposed in [11] is given by

$$\theta_i = \exp\left(\frac{2\pi j c_i^s}{N\Delta}\right) \quad s = 0,\ 1, \ldots, N-1. \tag{20}$$

with Δ being constellation dependent and is selected so as to make $2\pi/\Delta$ the minimum angle which rotates the transmit symbol alphabet onto itself ($\Delta = 2$ for the case of BPSK). Table 5 lists the characteristics of the different pairwise error classes for Walsh-Hadamard spreading and its rotated version for a group size of four BPSK symbols ($S = 4$). In contrast to conventional Walsh-Hadamard which attains $\hat{D}_{min} = 1$, for rotated Walsh-Hadamard spreading, all classes are characterized by $\hat{D}_c = \hat{D}_{min} = 4$. Taking into account the asymptotic BER expression in (17), this indicates that while using conventional Walsh-Hadamard spreading no diversity gain will be achieved, the rotated spreading has the potential (depending on the channel correlation matrix R) to attain a diversity gain equal to the number of employed subcarriers. Notice that, logically, in both cases there are the same number of different pairwise errors ($240 = 4^2 \times 4^2 - 4^2$). We conclude this section by remarking that here, only the maximization $\hat{D}_{min}$ has been pursued. Maximization of the product of eigenvalues $\{\hat{\lambda}_{\hat{D}_{min},d}\}_{d=1}^{\hat{D}_{min}}$ is a topic of current research.

Table 1. Ranks and number of entries of the different PEP classes

Walsh-Hadamard				Rotated Walsh-Had.			
$W(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c, i)$	$\hat{D}_c$	i	$\hat{\boldsymbol{\lambda}}_c$	$W(\hat{D}_c, \hat{\boldsymbol{\lambda}}_c, i)$	$\hat{D}_c$	i	$\hat{\boldsymbol{\lambda}}_c$
8	1	4	[64]	64	4	1	[3.29 3.39 4.25 5.07]
32	2	2	[15.09 16.91]	32	4	2	[10.13 8.51 6.58 6.78]
64	2	2	[14.06 17.93]	64	4	2	[2.17 2.36 14.5 12.92]
64	4	1	[3.29 3.39 4.25 5.07]	64	4	3	[23.78 13.14 10.42 0.66]
64	4	3	[3.33 3.81 4.7 36.14]	4	16	4	[30.74 24.8 5.11 4.06]
8	4	4	[13.16 13.55 17.01 20.24]				
$\Sigma = 240$				$\Sigma = 240$			

6 Numerical Results

We assume a system operating around 5 GHz with a total bandwidth of 100 MHz, such parameters are typically used in 4G systems currently under discussion (see for example [12]). The number of total subcarriers, N_{total}, is fixed to 2048 ensuring that each subcarrier undergoes frequency flat fading. The power delay profile of the ETSI BRAN channel A (typical office environment) has been used. This channel has 18 independent Rayleigh fading paths with an rms delay spread of 50 ns.

Figure 3 shows the simulation (circles) and analytical results (solid lines) when using different number of subcarriers in combination with conventional Walsh-Hadamard spreading. It is seen how the theoretical upper-bound provides an accurate approximation of the true BER for E_s/N_0 ratios of practical interest. Notice that the more subcarriers being used, the looser the bound is for low E_s/N_0 levels. This behavior is typical in analysis based on the union bound.

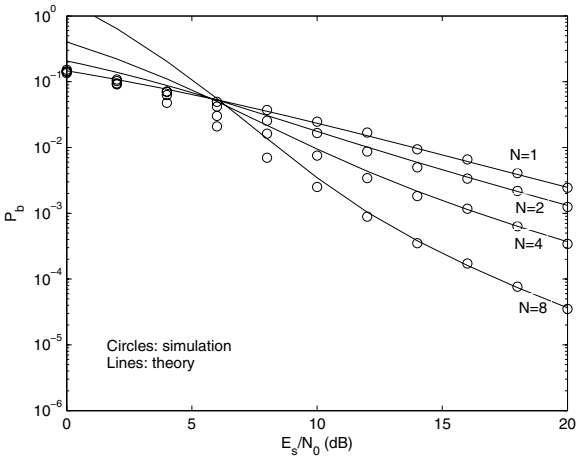


Fig. 3. BER when using N=1, 2, 4 and 8 subcarriers. Full load ($N = S$). Walsh-Hadamard spreading. BPSK modulation.

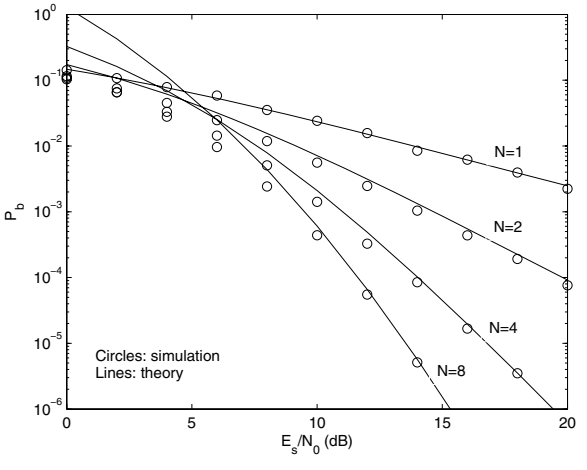


Fig. 4. BER when using N=1, 2, 4 and 8 subcarriers. Full load ($N = S$). Rotated Walsh-Hadamard spreading. BPSK modulation.

It can also be seen that, when using conventional Walsh-Hadamard spreading, increasing the number of subcarriers per group brings along a reduction in BER, however, it is already hinted in this figure that the asymptotic slope of the BER curves when using different number of subcarriers is the same. It has been shown in Section 5 that Walsh-Hadamard codes of length 4 induce $\hat{D}_{min} = 1$. Indeed this is also the case for any other code length. It is seen in Fig. 3 that, as predicted by the asymptotic analysis in Section 4, all curves tend to have a asymptotic slope of one (for $N = 8$ this holds at around $E_s/N_0 = 40$ dB).

Figure 4 presents the same set of simulations but now using rotated Walsh-Hadamard spreading. Again, good agreement can be observed between simulation (circles) and analytical (solid lines) results. The improvement with respect to conventional spreading is very clear. As an example, for $N = 4$, the rotated spreading provides a 4 dB gain with respect to the non-rotated one for $P_b = 10^{-3}$, for lower P_b's gains are even larger. It was shown in Section 5 that with the rotated spreading and $N = 4$, all pairwise error classes had $\hat{D}_c = \hat{D}_{min} = 4$ maximizing the achievable diversity order for a given channel correlation matrix and a specific number of subcarriers per group. It can indeed be seen in Fig. 4 that the BER curve for $N = 4$, at large E_s/N_0 levels, has a diversity order equal to four in agreement with the asymptotic prediction.

7 Conclusions

A new scheme, which we call group-orthogonal multicarrier code-division multiplex (GO-MC-CDM), suitable for the downlink segment of fourth generation of wireless communication systems has been proposed. This scheme allows the efficient use of multi-symbol detection schemes and offers the same performance as (downlink) GO-MC-CDMA at a fraction of its computational cost. The performance of this system has been analyzed when using maximum likelihood multi-symbol detection. A closed-form BER expression has been derived which reveals which are the important parameters to be taken into account in order to optimize the BER performance. In particular, choosing the subcarriers for a group to be equispaced over the whole available bandwidth and selecting a family of rotated spreading codes prove to be of fundamental importance in the minimization of the BER. Simulation results have also been presented validating the analytical derivations.

Acknowledgments

This work has been supported in part by the MEC and FEDER under project MARIMBA (TEC2005-0997) and a Ramon y Cajal fellowship, Spain.

References

1. N. Yee, J.-P. Linnartz, and G. Fettweis, "Multi-carrier CDMA in indoor wireless radio networks," in *Proc. IEEE Int. Symp. on Pers., Indoor and Mob. Rad. Comm.*, Yokohama (Japan), Sept. 1993, pp. 109–113.
2. S. Hara and R. Prasad, "Overview of multicarrier CDMA," *IEEE Communications Mag.*, vol. 35, pp. 126–133, December 1997.
3. K. Fazel and S. Kaiser, *Multi-Carrier and Spread Spectrum Systems.* Wiley, 2003.
4. X. Cai, S. Zhou, and G. Giannakis, "Group-orthogonal multicarrier CDMA," *IEEE Trans. Communications*, vol. 52, no. 1, pp. 90–99, January 2004.
5. S. Kaiser, "OFDM code-division multiplexing in fading channels," *IEEE Trans. Communications*, vol. 50, pp. 1266–1273, 2002.

6. J. Proakis, *Digital Communications*, 3rd ed. Mc-Graw Hill, 1996.
7. B. Hochwald and S. ten Brink, "Achieving near-capacity on a multiple-antenna channel," *IEEE Trans. Communications*, vol. 51, pp. 389–399, 2003.
8. J. W. Craig, "A new, simple and exact result for calculating the probability of error for two-dimensional signal constellations," in *IEEE MILCOM'91 Conf. Rec.*, Boston, MA, 1991, pp. 25.5.1–25.5.5.
9. M. Schwartz, W. Bennett, and S. Stein, *Communications Systems and Techniques.* Wiley-IEEE Press, 1995.
10. G. Femenias, "BER performance of linear STBC from orthogonal designs over MIMO correlated nakagami-m fading channels," *IEEE Trans. Vehicular Tech.*, vol. 53, pp. 307–317, 2004.
11. A. Bury, J. Egle, and J. Lindner, "Diversity comparison of spreading transforms for multicarrier spread spectrum transmission," *IEEE Trans. Communications*, vol. 51, no. 5, pp. 774–781, May 2003.
12. "European union framework program 6 - WINNER project," https://www.ist-winner.org/.

Performance Characterization of UWB SSMA Using Orthogonal PPM-TH in Dense Multipath

Fernando Ramírez-Mireles

Instituto Tecnológico Autónomo de México (ITAM)
Río Hondo 1, Col. Tizapán San Angel,
México City, D.F. C.P. 01000, México
ramirezm@ieee.org
http://www.geocities.com/f_ramirez_mireles

Abstract. In this work we study ultra wideband (UWB) communications over dense multipath channels using orthogonal pulse position modulation (PPM) for data modulation and time-hopping (TH) for code modulation. We consider the effects of the multiple access interference (MUI) in asynchronous spread spectrum multiple access (SSMA) based on random TH codes. We consider a realistic multipath channel to analyze the effects of the transmission rate in the number of users for different bit error rate (BER) values.

Keywords: Ultra wideband communications, pulse position modulation, multipath channels, spread spectrum multiple access.

1 Introduction

The UWB communications for short-range high-speed wireless communications has been studied extensively [1]-[7]. This work studies the performance of binary UWB communications in the presence of additive white Gaussian noise (AWGN), MUI, and dense multipath effects (DME). Several authors have studied this problem before.

The work in [8] studied an *all-digital* receiver using time hopping with binary pulse amplitude modulation and synchronous time-division duplexing, with a multipath channel model that assumes the path arrival times being uniformly distributed over the delay spread span and the amplitude of each path being Gaussian decaying linearly with delay, and with the maximum delay spread fixed to a certain constant value.

The work in [9] studied a *digital* receiver using TH combined with orthogonal binary PPM including *multi-stage block-spreading* to cancel MUI deterministically, with the channel modeled with a finite impulse response filter of fixed order that includes asynchronisms in the form of delay factors and frequency selective multipath effects.

The work in [10] used a signal-to-interference analysis to study the degradation factor due to MUI in the presence of DME when using binary PPM-TH signals, with a multipath model assuming path arrival times uniformly distributed over

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 401–412, 2006.

one frame period with special cases of exponentially decaying and flat amplitude profiles.

In [11] the error probability of UWB SSMA using TH combined with binary PPM is studied in the presence of interference and multiptah, comparing performance for different modulation schemes, interference conditions, and receivers types.

In [12] a closed-form expression of the MUI variance in multipath channel for binary pulse amplitude modulation and time hopping PAM-TH was found.

In this work we use a simple expression for the BER [13] and consider a realistic multipath indoor office channel using the Time Domain Corporation Indoor Channel Database to analyze the effects of the transmission rate in the number of users for different BER values.

2 System Model

2.1 Transmitted Signals

The *transmitted* signal is described by

$$\Psi_{\text{TX}}^{(\nu)}(t) = \sum_{k=0}^{N_s-1} p_{\text{TX}}(t - kT_f - c_k^{(\nu)}T_c - b_j\delta) \,, \tag{1}$$

where t denotes time, the index k is the number of time hops that the signal $\Psi_{\text{TX}}^{(\nu)}(t)$ has experienced, T_f is the average frame time between pulse transmissions, and $p_{\text{TX}}(t)$ is the UWB pulse used to build the transmitted PPM signals.

The superscript $1 \leq \nu \leq N_u$, indicates user-dependent quantities, Without loss of generality, we will assume that user one is the desired user.

The b_j is the j^{th} data bit, $j = 1, 2$, taking one of two equally likely values from the binary set $\{0, 1\}$. The time shift value δ is chosen such that set of signals are orthogonal in the absence of multipath.

For a given time shift parameter T_c, the pseudo-random TH code $\{c_k^{(\nu)}\}$ provides an additional time shift to the pulse in every frame, each time shift being a discrete time value $c_k^{(\nu)}T_c$, with $0 \leq c_k^{(\nu)}T_c < N_hT_c$. The data bit changes only every N_s hops, i.e., the system uses fast time hopping.

The UWB pulse $p_{\text{TX}}(t)$ is the basic signal used to convey information. This pulse is characterized by a radiated spectrum with a very wide bandwidth (a few Giga Hertz) around a relatively low center frequency (one or two Gigahertz). The duration of the pulse T_p is in the order of a few nanoseconds.[1]

[1] As defined by the Federal Communications Commission (FCC) of the United States, any signal is of UWB nature when it has a 10 dB bandwidth of at least 500 MHz, or when its fractional bandwidth (the ratio of the 10 dB bandwidth to the central frequency) is at least 20 percent [14].

2.2 Model for the Gaussian Channel

Under free space propagation conditions the received signal

$$\Psi^{(\nu)}(t) = \sum_{k=0}^{N_s-1} p(t - kT_f - c_k^{(\nu)} T_c - b_j \delta) \tag{2}$$

is modeled as the derivative of the transmitted signal $\Psi_{\text{TX}}^{(\nu)}(t)$.[2] The received signal is modified by amplitude A_o and delay τ_o factors that depend on the transmitter-receiver separation distance (in our analysis we will assume $A_o = 1$ and $\tau_o = 0$).

The signals $\Psi^{(\nu)}(t)$ in (2) have duration $T_s = N_s T_f$ and energy

$$E_\Psi \triangleq \int_{-\infty}^{\infty} [\Psi^{(\nu)}(t)]^2 dt = N_s E_p \ , \tag{3}$$

for $j = 1, 2$, where $E_p = \int_{-\infty}^{\infty} [p(t)]^2 dt$ is the energy of the *received* UWB pulse $p(t)$. The signals $\Psi^{(\nu)}(t)$ have normalized correlation values

$$\beta \triangleq \frac{\int_{-\infty}^{\infty} \Psi_{j_1}^{(\nu)}(t)\, \Psi_{j_2}^{(\nu)}(t)\, dt}{E_\Psi} = \begin{cases} 1, & j_1 = j_2 \ , \\ \gamma(\delta), & j_1 \neq j_2 \ , \end{cases} \tag{4}$$

where

$$\gamma(\delta) \triangleq \frac{\int_{-\infty}^{\infty} p(t)\, p(t-\delta)\, dt}{E_p} \tag{5}$$

is the normalized autocorrelation function of $p(t)$. The time shift value $\delta = 2T_p$ is chosen such that the signal correlation $\gamma(\delta) = 0$.

The noise at the receiver $n(t)$ is AWGN with two-sided power spectrum density (PSD) $N_o/2$.

2.3 Model for the Multipath Channel

Multiple-Path Trajectories. For each active link the corresponding transmitter stays fixed at certain arbitrary position, and the corresponding receiver moves in a spatially random fashion.

In particular, the link between user one's receiver and user ν's transmitter defines a multiple-path propagation trajectory that is a function of the relative position of user one's receiver with respect to the position of user ν's transmitter. This random trajectory will be identified with the random index $\xi^{(\nu)}$. There will be N_u of such trajectories, one for every pair (user ν's transmitter, user one receiver), $\nu = 1, 2, \ldots, N_u$.

[2] This model for the antenna system has been repeatedly used [1]-[7]. Most existing UWB antennas do not have the differentiation effect. Even for those antennas systems, the analysis in this work still can be applied because it is based on the energy and correlation values of the *received* signals.

When user ν's transmitter radiates the signal $p_{\text{TX}}(t)$, the signal detected by user one's receiver will be represented by $p(\xi^{(\nu)}, t)$. As we move user one's receiver position, these trajectories change. Hence, the received waveforms coming from each of the transmitters also change.

Channel Effect in the UWB Pulse. In an indoor multipath channel, transmission of the pulse $p_{\text{TX}}(t)$ results in a received "pulse" $\sqrt{E_a}\, p(\xi^{(\nu)}, t)$ which is is a multipath spread version of $p(t)$. The average duration of $p(\xi^{(\nu)}, t)$ is denoted T_a, and can be in the order of up to a few hundreds of nanosecond, hence $T_a >> T_p$. We will assume that T_a is the equivalent of the mean delay spread of the channel.

The pulse $\sqrt{E_a}\, p(\xi^{(1)}, t)$ has random energy $E_p(\xi^{(1)}) \triangleq E_a\, \alpha^2(\xi^{(1)})$, where E_a is the average received energy, and $\alpha^2(\xi^{(1)}) \triangleq \int_{-\infty}^{\infty} [p(\xi^{(1)}, t)]^2 dt$ is the normalized random energy. The pulse has normalized random signal correlation

$$\gamma(\xi^{(1)}, \delta) \triangleq \frac{\int_{-\infty}^{\infty} p(\xi^{(1)}, t)\, p(\xi^{(1)}, t - \delta)\, dt}{\alpha^2(\xi^{(1)})} \, .$$

The normalized signal cross-correlation corresponding to pulses received with two different trajectories $\xi^{(1)}$ and $\xi^{(\nu)}$ is

$$\tilde{\gamma}(\xi^{(1)}, \xi^{(\nu)}, \delta) \triangleq \frac{\int_{-\infty}^{\infty} p(\xi^{(1)}, t)\, p(\xi^{(\nu)}, t - \delta)\, dt}{\tilde{\alpha}^2(\xi^{(1)}, \xi^{(\nu)})} \, ,$$

where $\tilde{\alpha}^2(\xi^{(1)}, \xi^{(\nu)}) \triangleq \int_{-\infty}^{\infty} p(\xi^{(1)}, t)\, p(\xi^{(\nu)}, t)\, dt$.

2.4 Model for the Multipath Channel

The PPM-TH signals received in the presence of multipath are

$$\Psi^{(\nu)}(\xi^{(\nu)}, t) = \sum_{k=0}^{N_s - 1} \sqrt{E_a} p(\xi^{(\nu)}, t - kT_f - c_k^{(\nu)} T_c - b_j \delta) \, . \tag{6}$$

The signal in (6) is received with trajectory $\xi^{(\nu)}$, and is a multipath spread version of the signal in (2).

Here we have assumed that the channel is slowly time invariant, therefore the PPM signal is composed of shifted version of the same spreaded pulse. We will further assume that $\Psi^{(\nu)}(\xi^{(\nu)}, t)$ has fixed duration $T_s \simeq N_s T_f$.

The signals $\Psi^{(1)}(\xi^{(1)}, t)$ have random energy

$$E_\Psi(\xi^{(1)}) = \int_{-\infty}^{\infty} [\Psi^{(1)}(\xi^{(1)}, t)]^2 dt \simeq \overline{E}_s \alpha^2(\xi^{(1)}), \tag{7}$$

where $\overline{E}_s = N_s E_a$ is the average bit energy. The signals have normalized random correlation values

$$\beta(\xi^{(1)}) \triangleq \frac{\int_{-\infty}^{\infty} \Psi_{j_1}^{(1)}(\xi^{(1)}, t)\, \Psi_{j_2}^{(1)}(\xi^{(1)}, t)\, dt}{E_\Psi(\xi^{(1)})} = \begin{cases} 1, & j_1 = j_2 \, , \\ \gamma(\xi^{(1)}, \delta), & j_1 \neq j_2 \, , \end{cases} \tag{8}$$

2.5 The Case with Multiple-Users

In the system model under consideration all the users transmit the same type of binary time hopping PPM signals in (1) to convey information, the difference being the TH code used for each user. Also, all the users experience the same multipath environment, although each one has its own multipath trajectory. When N_u asynchronous transmitters are active, the received signal at user one's receiver position is modeled as

$$r(t) = \sum_{\nu=1}^{N_u} A^{(\nu)} \Psi^{(\nu)}(\xi^{(\nu)}, t - \tau^{(\nu)}) + n(t) \; , \tag{9}$$

where $\tau^{(\nu)}$ represent time asynchronisms between the clock of user ν's transmitter and user one's receiver, $(A^{(\nu)})^2$ is the ratio of average power used by user ν's transmitter with respect to the average power used by user one's transmitter (with $(A^{(1)})^2 = 1$), and $n(t)$ represents non MUI interference modeled as AWGN.

The signal $r(t)$ in (9) is a random process that depends on the random noise $n(t)$ and three other types of random variables: The random time delays, denoted by the vector $\underline{\tau} = (\tau^{(2)}, \tau^{(3)}, \ldots, \tau^{(N_u)})$; the random time hopping codes, denoted by the vector $\underline{C} = (C^{(2)}, C^{(3)}, \ldots, C^{(N_u)})$, where each code $C^{(\nu)} = \{c_k^{(\nu)}\}$ for $k = 0, 1, \ldots, N_s - 1$; and the random multiple-path trajectories indexes, denoted by $\xi^{(1)}$ and the vector $\underline{\xi} = (\xi^{(2)}, \xi^{(3)}, \ldots, \xi^{(\nu)})$. Performance computation is based on signal-to-interference (SIR) ratios and BER rates averaged over all random variables.

To facilitate our analytical treatment, the following assumptions are made

1. We can treat $\xi^{(\nu)}$, $\nu = 1, 2, \ldots, N_u$, as independent, identically distributed (i.i.d.) random variables, with each $\xi^{(\nu)}$ uniformly distributed over its range. The expected values with respect to $\xi^{(\nu)}$ can be approximated with sample averages based on parameters calculated using measured or synthesized received waveforms as in [15]. The $\int_{-\infty}^{\infty} p(\xi^{(\nu)}, t)dt \simeq 0$.
2. The receiver is able to perfectly match user one's received signal, and it will be assumed to be perfectly synchronized.
3. Since $\delta << T_f$ we will assume $\delta = 0$ for $\nu = 2, 3, \ldots, N_u$.
4. The elements of the TH code are i.i.d random variables. Each $c_k^{(\nu)}$ is uniformly distributed on the interval $[0, N_h]$. We don't specify N_h because the assumption 6) produce results independent of it.
5. The transmission time differences $\tau^{(\nu)} - \tau^{(1)} \stackrel{\triangle}{=} \Phi^{(\nu)} T_f + \phi^{(\nu)}$, for $\nu = 2, \ldots, N_u$, are i.i.d random variables, with $\phi^{(\nu)} \stackrel{\triangle}{=} \tau^{(\nu)} - \tau^{(1)} \bmod T_f$ being uniformly distributed on $[0, T_f]$, where mod means the modulus operation. We don't characterize $\Phi^{(\nu)}$ because results will be independent of it.
6. To avoid overlapping of pulses belonging to different frames in (1) the maximum time shift produced by the TH code is limited to $N_h T_c < ((T_f - T_a)/2) - \epsilon$, where $\epsilon \stackrel{\triangle}{=} 2(T_p + \delta)$. Combining this condition, together with

$T_f > (T_a + \delta)$, we can ensure that both inter-pulse and inter-symbol interference can be neglected.

With these assumptions the net effect of the multiple access interference at the output of the demodulation circuit can be modeled as a zero mean Gaussian random variable (r.v.).[3]

3 Receiver Signal Processing and Performance

To simplify notation, in the following analysis we will drop the super-index $^{(1)}$ from $\Psi^{(1)}(\xi^{(1)}, t)$, $A^{(1)}$, $\tau^{(1)}$, and $c^{(1)}$.

3.1 Signal Detection

Let's assume that the receiver wants to demodulate user one's signal. The received signal $r(t)$ in (9) can be rewritten

$$r(t) = A\Psi(\xi, t-\tau) + n_{\text{TOT}}(t),\ t \in \mathcal{T}\ , \tag{10}$$

where $\mathcal{T} \triangleq [\tau, N_s T_f + \tau]$, and

$$n_{\text{TOT}}(t) \triangleq \sum_{\nu=2}^{N_u} A^{(\nu)}\Psi^{(\nu)}(\xi^{(\nu)}, t-\tau^{(\nu)}) + n(t)\ .$$

For the time being, let's assume that user one's receiver is static at one place, and that user one's transmitter is at a fixed position, i.e., ξ is kept fixed.

In the present analysis signal detection is achieved using a Rake receiver [17]. For binary communications a perfectly synchronized rake Receiver will have 2 filters matched to $\Psi_j(\xi, t-\tau)$, $j = 1, 2$. The output of the j^{th} matched filter

$$y_j = \int_{t\in\mathcal{T}} r(t)\,\Psi_j(\xi, t-\tau)dt \triangleq y_s + y_m + y_n\ , \tag{11}$$

can be seen as the sum of three outputs: the output y_s of a filter perfectly matched and synchronized to the signal, the output y_m of a filter mismatched and asynchronous to the interference, and the output y_s consisting of filtered noise.

The signal term y_s takes into account the correlation of the desired user with itself

$$y_s = \int_{t\in\mathcal{T}} A\,\Psi(\xi, t-\tau)\,\Psi_j(\xi, t-\tau)dt = \begin{cases} E_\Psi(\xi), & \text{for } \Psi(\cdot) = \Psi_j(\cdot)\ , \\ E_\Psi(\xi)\,\beta(\xi), & \text{for } \Psi(\cdot) \neq \Psi_j(\cdot)\ , \end{cases} \tag{12}$$

[3] For the case under study, i.e., signals with several pulses per bit N_s, the Gaussian approximation for the effect of the MUI at the output of the correlator is justified by the central limit theorem for various users Nu, and has been used repeatedly by several authors. In particular, the results in [16] shows that for the values of N_s and N_u considered here the MUI effects can be modeled as produced by a Gaussian r.v.

The multiple-access term y_m takes into account the cross-correlation among user one and the interfering users

$$y_m = \int_{t\in\mathcal{T}} \sum_{\nu=2}^{N_u} A^{(\nu)}\, \Psi^{(\nu)}(\xi^{(\nu)}, t-\tau^{(\nu)})\, \Psi_j(\xi, t-\tau)\, dt$$
$$= \sum_{\nu=2}^{N_u} \sum_{k=0}^{N_s-1} A^{(\nu)} E_a \tilde{\alpha}^2(\xi, \xi^{(\nu)}, \tau^{(\nu)}) \tilde{\gamma}(\xi, \xi^{(\nu)}, \Omega_k^{(\nu)} - \phi^{(\nu)} - (b_{j_1} - b_j)\delta) \quad (13)$$

where $\Omega_k^{(\nu)} \triangleq c^{(\nu)}_{k-\Phi^{(\nu)}} - c_k$.

Finally, the noise term is

$$y_n = \int_{t\in\mathcal{T}} n(t)\, \Psi_j(\xi, t-\tau)\, dt\ . \quad (14)$$

3.2 Performance Conditioned on ξ

The performance of such correlation receiver can be analyzed using traditional detection theory [18],[4] and the demodulation problem can be analyzed as the time-shift-coherent detection of M equal-energy, equally-likely signals in the presence of Gaussian interference plus noise using a binary correlation receiver. The resulting performance results should be considered as a lower bound, i.e., performance of an ideal Rake receiver.

The BER is given by

$$\mathrm{UBPe}(N_u|\xi) = \frac{M}{2} \int_{\sqrt{\mathrm{SIR}_{\mathrm{out}}(N_u|\xi)}}^{\infty} \frac{\exp(-\rho^2/2)}{\sqrt{2\pi}}\, d\rho, \quad (15)$$

where

$$\mathrm{SIR}_{\mathrm{out}}(N_u|\xi) \triangleq \frac{1}{\left[\mathrm{SIR}_{\mathrm{out}}(1|\xi)\right]^{-1} + \left[\mathrm{SIR}_{\mathrm{MUI}}(N_u|\xi)\right]^{-1}}\ , \quad (16)$$

is the output bit SIR observed in the presence of $N_u - 1$ other users and, for the time being, is being conditioned on ξ. The

$$\mathrm{SIR}_{\mathrm{out}}(1|\xi) \triangleq \frac{E_s\, \alpha^2(\xi)\, [1-\beta(\xi)]}{N_o} \quad (17)$$

is the bit SNR in the presence of AWGN and in the absence of MUI, and

$$\mathrm{SIR}_{\mathrm{MUI}}(N_u|\xi) \triangleq \frac{E_s\, \alpha^2(\xi)\, [1-\beta(\xi)]}{N_{\mathrm{MUI}}(\xi)} \simeq \frac{\mathcal{G}(\xi)}{N_u}\ , \quad (18)$$

is the bit SNR in the presence of MUI and in the absence of AWGN, where $N_{\mathrm{MUI}}(\xi)$ is the *equivalent* PSD level of the total MUI, and where $\mathcal{G}(\xi) \triangleq \frac{\mu(\xi)}{T_f \mathcal{R}_\downarrow}$ is

[4] Since the MUI is modeled as Gaussian noise, this correlation receiver is sub-optimum, the optimum receiver being a multi-user detector [19].

a *random* processing gain factor, where $R_b = 1/T_s$ is the bit transmission rate, and where

$$\mu(\xi) = \frac{m_p^2(\xi, \xi, 0, 0, \delta)}{\mathbf{E}_{(\xi^{(\nu)}|\xi)}\{\int_{-\infty}^{\infty} m_p^2(\xi, \xi^{(\nu)}, \varsigma, 0, \delta)\, d\varsigma\}} \tag{19}$$

is a normalized random SIR parameter defined in terms of both the received UWB pulse shape and the time-shift defining the orthogonal PPM data modulation, where $\mathbf{E}_{(\xi^{(\nu)}|\xi)}\{\cdot\}$ is the expected value with respect to $\xi^{(\nu)}$ conditioned on ξ, and where

$$\begin{aligned} m_p(\xi, \xi^{(\nu)}, \varsigma, 0, \delta) &\triangleq \int_{-\infty}^{\infty} p(\xi^{(\nu)}, \varrho)\ [p(\xi, \varrho) - p(\xi, \varrho - \delta)]\, d\varrho \\ &= \begin{cases} \alpha^2(\xi) \times \\ [\gamma(\xi, \varsigma) - \gamma(\xi, \varsigma - \delta)]\,, & \text{for } \nu = 1\,, \\ \\ \tilde{\alpha}^2(\xi, \xi^{(\nu)}) \times \\ \left[\tilde{\gamma}(\xi, \xi^{(\nu)}, \varsigma) - \tilde{\gamma}(\xi, \xi^{(\nu)}, \varsigma - \delta)\right]\,, & \text{for } \nu \neq 1\,, \end{cases} \end{aligned} \tag{20}$$

The averaged performance can be obtained by taking the expected value $\mathbf{E}_\xi\{\cdot\}$ of (15) over all values of ξ to get

$$\overline{\mathrm{UBPe}}\left(\frac{\overline{E}_s}{N_o}, N_u\right) = \mathbf{E}_\xi\{\mathrm{UBPe}\,(N_u|\xi)\}\,. \tag{21}$$

4 Numerical Results

4.1 UWB Pulse

In this numerical example the UWB pulse is the second derivative of a Gaussian pulse

$$p(t) = \left[1 - 4\pi\left[\frac{t}{t_n}\right]^2\right] \exp\left(-2\pi\left[\frac{t}{t_n}\right]^2\right), \tag{22}$$

for $-T_p/2 \leq t \leq T_p/2$, where t_n is a parameter that determine the pulse duration. The pulse energy $E_p = 3t_n/8$. For this pulse the signal correlation function is

$$\gamma(\tau) = \left[1 - 4\pi\left[\frac{\tau}{t_n}\right]^2 + \frac{4\pi^2}{3}\left[\frac{\tau}{t_n}\right]^4\right] \exp\left(-\pi\left[\frac{\tau}{t_n}\right]^2\right), \tag{23}$$

for $-T_p \leq \tau \leq T_p$.

For $t_n = 0.7531$ ns we get a pulse duration $T_p \simeq 2.0$ ns. In this case the spectrum of $p(t)$ is centered at about 1.1 GHz, with a 3 dB bandwidth of about 1.2 GHz, easily satisfying the traditional definition of UWB signal stating that the 10 dB bandwidth of the signal should be at least 20 percent of its center frequency [14]. Fig. 1 shows this pulse.

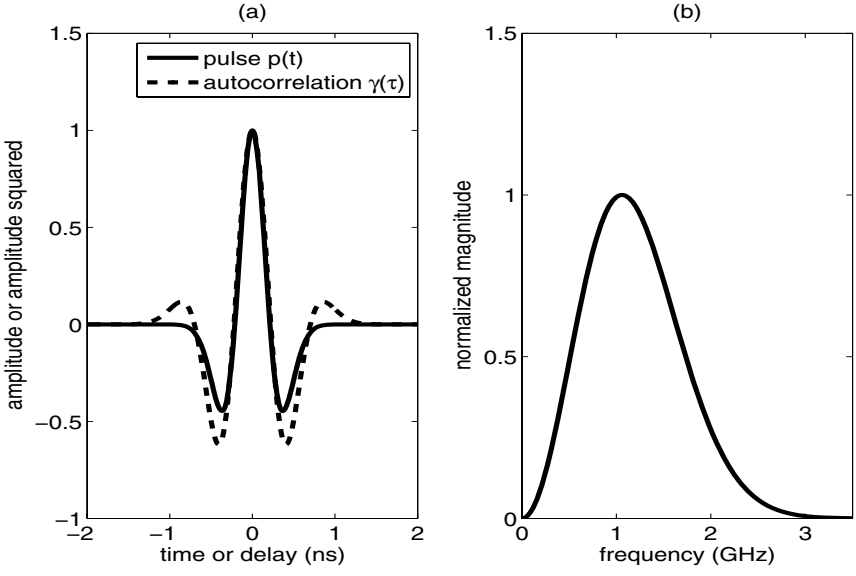


Fig. 1. The plots for (a) $p(t)$, (b) $\gamma(\tau)$, and (c) the spectrum of $p(t)$

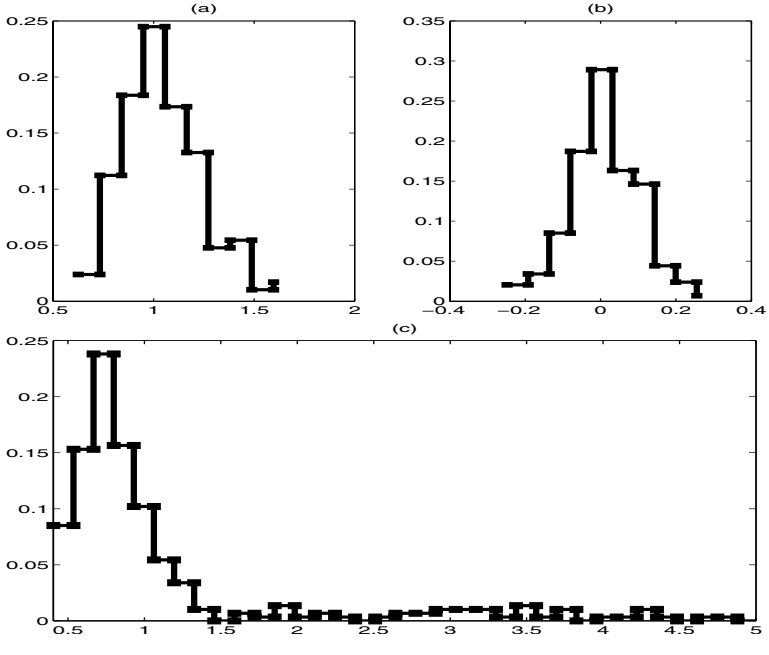


Fig. 2. The histograms for (a) $\alpha^2(\xi)$, (b) $\beta(\xi)$, and (c) $\mu(\xi)$. The ordinate represents appearance frequency, and the abscissa represents the value of the parameter.

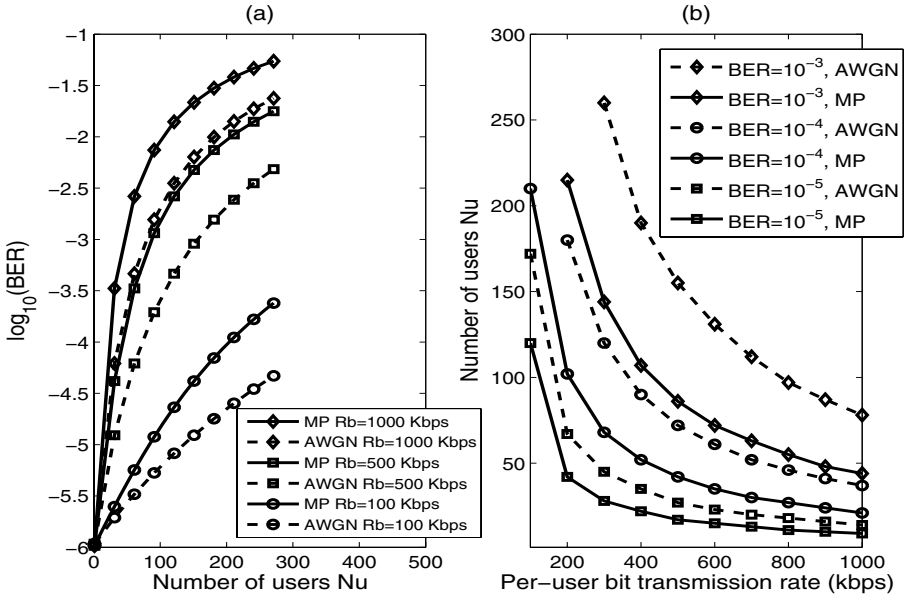


Fig. 3. (a) BER vs. number of users for different R_b. (b) Number of users to preserve BER for a given R_b.

The set of $p(\xi^{(\nu)}, t)$ were taken from the Time Domain Corporation Indoor Channel Database, available at USC's ULTRA-LAB WEB site at $http://click.usc.edu/New\_Site/database.html$. These UWB "pulses" have an average delay spread $T_a \simeq 300$ ns.

4.2 Calculations

For this example we use $T_f = 350$ ns and $R_b = 100$ to $R_b = 1000$ kilobits per second (Kbps) per user. For the Gaussian case we use $\alpha^2 = 1$ and $\beta = 0$ and calculate $\mu \simeq 1.3$. For the multipath case fig. 2 depicts histograms for $\alpha^2(\xi)$, $\beta(\xi)$ and $\mu(\xi)$.

Fig. 3(a) shows BER vs. Nu for $R_b = 100, 500, 1000$ kbps. Fig. 3(b) shows the number of users Nu to preserve a BER value for $R_b = 100$, 200, 300, 400, 500, 600, 700, 800, 900, 1000 Kbps.[5]

5 Conclusions

In this work we study UWB SSMA based on PPM-TH. We analyze the effects of the transmission rate in the number of users for different BER.

[5] Similar to [15], the calculations for the multipath case are based on sample averages over the different realizations of $\alpha^2(\xi)$, $\beta(\xi)$ and $\mu(\xi)$ considering a sample size of 49 for every room, and averaging the results over 5 rooms.

Fig. 3(b) shows the number of users Nu to preserve a BER value for different values of R_b in Kbps. For the BER and SIR values in Fig. 3(a), $\mathrm{SIR}_{\mathrm{MUI}}(N_u|\xi)$ dominates over $\mathrm{SIR}_{\mathrm{out}}(1|\xi)$ and therefore $N_u \simeq \frac{1}{\mathrm{SIR}_{\mathrm{out}}(N_u|\xi)} \frac{\mu(\xi)/T_f}{R_b}$.

For the type of signals and indoor office channel under consideration, these result indicate the following:

- For BER=10^{-5}, e.g., in data applications requiring low BER, the number of simultaneous radio links decreases from more than 100 to less than 10 when R_b goes from 100 kbps to 1000 kbps. This corresponds to a decrease in a factor in the order of 10 in the processing gain.
- For BER=10^{-3}, e.g., in voice applications requiring low BER, the number of simultaneous radio links decreases from more than 200 to less than 50 when R_b goes from 300 kbps to 1000 kbps. This corresponds to a decrease in a factor in the order of 3.4 in the processing gain.
- To obtain a combination with $N_u \geq 100$ users, $R_b \geq 1$ Megabits per second, and BER$\leq 10^{-5}$, some form of forward error correction must be used.

References

1. R. A. Scholtz, Multiple Access with Time Hopping Impulse Modulation, invited paper, in Proc. IEEE MILCOM Conf. (1993), pp. 447-450.
2. P. Withington II and L. W. Fullerton, An impulse radio communications system, in Ultra-Wideband, Short-Pulse Electromagnetics, H. L. Bertoni, L. Carin and L. B. Felson, Ed. New York: Plenum Press (1993), pp. 113-120.
3. M.Z. Win and R.A. Sholtz,Ultra-Wide Bandwidth Time-Hopping Spread-Spectrum Impulse Radio for Wireless Multiple-Access Communication, IEEE Trans. Commun., Vol. 48 (2000), pp. 679-691.
4. F. Ramírez-Mireles, Performance of Ultrawideband SSMA Using Time Hopping and binary PPM, IEEE J. Select. Areas Commun., Vol. 19 (2001), pp. 1186-1196.
5. Special Issue on UWB - State of the art, EURASIP JASP., Vol. 2005, no. 3 (2005).
6. Special Issue on UWB Wireless Communications - A new Horizon, IEEE Trans. on Veh. Tech., Vol. 54, no. 5 (2005).
7. R. C. Qiu, H. Liu, X. Shen,, Ultra-Wideband for Multiple Access Communications, in IEEE Commun. Magazine, Vol. 43, No. 2 (2005), pp. 2-8.
8. C.J. Le Martret and G.B. Giannakis, All-Digital PAM Impulse Radio for Multiple-Access Through Frequency-Selective Multipath, in Proc. IEEE GLOBECOM Conf. (2000), pp. 77-81.
9. L Yang and G.B. Giannakis, Impulse Radio Multiple Access Through ISI Channels with Multi-Stage Block-Spreading, in Proc. IEEE UWBST Conf. (2002), pp. 277-282.
10. A. Taha and K. M. Chugg, Multipath Diversity Reception of Wireless Multiple Access Time-Hopping Digital Impulse Radio, in Proc. IEEE UWBST Conf. (2002), pp. 283-288.
11. G. Durisi et al, A General Method for Error Probability Computation of UWB Systems for Indoor Multiuser Communications, in Journal of Communications and Networks, Vol. 5, no. 4 (2003), pp. 354-364.
12. C. J. Le Martret, A-L Deleuze, P. Ciblat, Optimal Time-Hopping Codes for Multi-User Interference Mitigation in Ultra-Wide Bandwidth Impulse Radio, in IEEE Trans. on Wireless Commun., to be published.

13. F. Ramírez-Mireles, Error Probability of Ultra Wideband SSMA in a Dense Multipath Environment, in Proc. IEEE MILCOM Conf. (2002).
14. U.S. Federal Communications Commission, First Report and Order for UWB Technology, U.S. Federal Communications Commission, April 2002.
15. F. Ramírez-Mireles, On Performance of Ultra Wideband Signals in Gaussian Noise and Dense Multipath, IEEE Trans. Veh. Technol., Vol. 50, no.1 (2001), pp. 244-249.
16. A. Almada and F. Ramírez-Mireles, Statistical Behavior of UWB TH-PPM MUI at the output of a single-correlator receiver, under review in *IEEE Trans. on Commun.*
17. J. G. Proakis, *Digital Communications,"* New York:McGraw-Hill, pp. 797-805,1995.
18. R. M. Gagliardi, Introduction to Telecommunications Engineering, John Wiley and Sons (1988).
19. E. Fishler and H. V. Poor, Low-Complexity Multiuser Detectors for Time-Hopping Impulse-Radio Systems, IEEE Trans. on Signal Processing, Vol. 52, no. 9 (2004), pp. 2561-2571.
20. C. L. Weber, G. K. Huth and B. H. Batson, Performance Considerations of Code Division Multiple-Access Systems, IEEE Trans. on Veh. Technol., Vol. 30, no. 1 (1981), pp. 3-9..

An Efficient Bit Loading for OFDM with Diversity Scheme over Mobile Channel

Tae Jin Hwang, Sang Soon Park, and Ho Seon Hwang

664-14, Duckjin-Dong 1Ga, Jeonju 561-756, Korea
Department of Electronic Engineering, Chonbuk National University
tjhwang@chonbuk.ac.kr

Abstract. This paper discusses an adaptive modulation technique combined with space-frequency block coded OFDM(SFBC OFDM) over frequency selective channels and evaluates the performance in terms of the outdated channel state information(CSI) in mobile environments. This paper employs the Alamouti's diversity scheme in multiple input multiple output OFDM (MIMO OFDM) and an adaptive modulation with enhanced performance. Adaptive modulation scheme shows very attractive performance when the CSI is perfect. The CSI for bit loading in MIMO OFDM can be obtained from the singular value decomposition(SVD) of MIMO channel. But, SFBC OFDM system based on Alamouti's diversity scheme does not require the SVD process. Through various simulations, the performance of SFBC OFDM employing adaptive modulation is compared with that of fixed modulation. Also, in adaptive modulation scheme, the effects of the outdated CSI under mobile environments are shown

1 Introduction

Recently, a considerable number of studies have been conducted on reliable high data rate services in broadband wireless communications. In frequency selective channel, some of mechanisms are required in order to combat the effects of intersymbol interference(ISI). Orthogonal frequency division multiplexing(OFDM) technique transforms a frequency selective channel into parallel correlated flat channels by increasing symbol duration. However, the performance of OFDM system could be degraded due to deep faded subchannels. For a better performance, the OFDM transmitter adapts the subchannel bit and power allocation to the amplitude response of the frequency selective channel[1].

On the other hand, the most popular technique has been the exploitation of diversity in order to overcome multipath fading in wireless environments. Alamouti discovered a remarkable space time block coded scheme using two transmit antennas in narrowband wireless communication [2]. The novel diversity scheme has been proved effectively in combating fading and has motivated various transmit diversity techniques. However, this is faced with a very complex equalization problem to overcome frequency-selective fading environments. Several studies have been made on transmit diversity technique in context of OFDM, such as space-time block coded OFDM (STBC OFDM) or space-frequency block coded OFDM(SFBC OFDM), and et al [3]~[5].

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 413 – 424, 2006.

In order to improve the performance of OFDM system in frequency selective and multipath fading environments, this paper presents an adaptive bit allocation combined with SFBC OFDM. The perfect CSI ensures a desired efficiency/ performance of adaptive modulation scheme. In MIMO OFDM system, by making use of SVD the MIMO channel on each subcarrier is decomposed into parallel non-interfering single input single output(SISO) channels. But, a SFBC OFDM system with Alamouti's diversity scheme does not require the SVD for the CSI. Assuming the availability of the perfect CSI at the transmitter, the performance gains of adaptive modulation have been demonstrated. This paper examines the impact on performance of an adaptive OFDM system, which combined with SFBC scheme, due to the outdated CSI in mobile fading channel. The organization of this paper is as follows. In section II, we will describe a system model and introduce SFBC OFDM in brief. In section III, we discuss the considered CSI for adaptive modulation in SFBC OFDM system and explain bit allocation method. In section IV, the performance of adaptive SFBC OFDM is evaluated under a variety of environment. Finally, a conclusion is made in Section V.

2 System Model and SFBC-OFDM

2.1 System Description

Fig.1 illustrates a block diagram of SFBC OFDM with adaptive modulation. To begin with, we assume that both the transmitter and the receiver perfectly know the channel state information. But, in mobile situation, the CSI will be outdated at the transmission time. In this paper, we consider the Alamouti's transmit diversity scheme applied to MIMO OFDM system with *N* tones, two transmit antennas and two receive antennas. At the transmitter, adaptive modulation based on the CSI is firstly performed. Two blocks of data through adaptive modulator are serial to parallel (S/P) converted. Two symbol vectors, $\mathbf{X}_1$ and $\mathbf{X}_2$, are coded by ST encoder. During the *n*-th symbol period, the symbol vector $\mathbf{X}_1$ will be transmitted from antenna one and $\mathbf{X}_2$ will be transmitted from antenna two. During next symbol period, $-\mathbf{X}_2^*$ will be

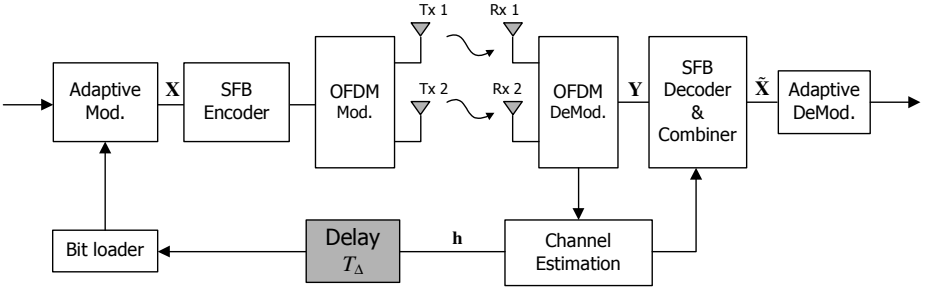


Fig. 1. Block diagram of an adaptive SFBC OFDM

transmitted from antenna one, and $\mathbf{X}_1^*$ will be transmitted from antenna two where $*$ is the complex conjugate operation. The respective vectors are synthesized by the inverse fast Fourier transform (IFFT). To avoid ISI, a cyclic prefix (CP) is inserted at the beginning of each OFDM frame as a guard interval, the length of which is at least as long as the maximum delay of two channels. Two signals are transmitted at a particular transmitter antenna during two time slots. The transmitted signal is faded by time varying channel and added noise. At the receiver, the transmitted symbols are sequentially restored through the maximal ratio combiner(MRC), maximum likelihood(ML) detector and adaptive demodulator.

2.2 Space Frequency Block Coded OFDM Scheme

This paper considers a MIMO OFDM system employing the Alamouti's diversity scheme. To begin with, let $\mathbf{X}(n)$ be the *n*-th transmit symbol as follows

$$\mathbf{X}(n) = [X(n,0)X(n,1) \cdots X(n,N-1)]^T \tag{1}$$

The data symbol vector $\mathbf{X}(n)$ is coded into two vectors $\mathbf{X}_1(n)$ and $\mathbf{X}_2(n)$ by the space-frequency encoder block as

$$\begin{aligned} \mathbf{X}_1(n) &= [X(n,0) \quad -X^*(n,1) \quad \cdots \quad X(n,N-2) \quad -X^*(n,N-1)]^T \\ \mathbf{X}_2(n) &= [X(n,1) \quad X^*(n,0) \quad \cdots \quad X(n,N-1) \quad X^*(n,N-2)]^T. \end{aligned} \tag{2}$$

At the *n* th block, $\mathbf{X}_1(n)$ is transmitted from the first base station Tx1 while $\mathbf{X}_2(n)$ is transmitted simultaneously from the second base station Tx2. The operations of the space frequency encoder/decoder can be described in terms of even and odd poly-phase component vectors. Let $\mathbf{X}_e(n)$ and $\mathbf{X}_o(n)$ be two vectors denoting the even and odd component vectors of $\mathbf{X}(n)$. Similarly, $\mathbf{X}_{1,e}(n)$ and $\mathbf{X}_{1,o}(n)$ denote the even and odd component vectors of $\mathbf{X}_1(n)$, i.e.,

$$\begin{aligned} \mathbf{X}_{1,e}(n) &= [X(n,0) \quad \cdots \quad X(n,N-2)]^T \\ \mathbf{X}_{1,o}(n) &= [-X^*(n,1) \quad \cdots \quad -X^*(n,N-1)]^T. \end{aligned} \tag{3}$$

Also, $\mathbf{X}_{2,e}(n)$ and $\mathbf{X}_{2,o}(n)$ denote the even and odd component vectors of $\mathbf{X}_2(n)$,i.e.,

$$\begin{aligned} \mathbf{X}_{2,e}(n) &= [X(n,1) \quad \cdots \quad X(n,N-1)]^T \\ \mathbf{X}_{2,o}(n) &= [X^*(n,0) \quad \cdots \quad X^*(n,N-2)]^T. \end{aligned} \tag{4}$$

Therefore, $\mathbf{X}_e(n)$ and $\mathbf{X}_o(n)$ can be expressed in terms of upper vectors as

$$\begin{aligned} \mathbf{X}_e(n) &= \mathbf{X}_{1,e}(n) = \mathbf{X}_{2,o}^*(n) \\ \mathbf{X}_o(n) &= \mathbf{X}_{2,e}(n) = -\mathbf{X}_{1,o}^*(n). \end{aligned} \tag{5}$$

Let $\mathbf{H}_{ij}(n)$ be the following diagonal matrix whose diagonal elements are the frequency responses of the channel impulse responses h_{ij} between the *i*-th transmit antenna and the *j*-th receive antenna during the *n*-th time slot

$$\mathbf{H}_{ij}(n) = \mathrm{diag}[H_{ij}(n,0) \cdots H_{ij}(n,N-1)], \quad i=1,2,\ j=1,2 \tag{6}$$

Let $\mathbf{Y}_j(n)$ be the *n*-th received OFDM symbol from the *j*-th receive antenna as follows

$$\mathbf{Y}_j(n) = \mathbf{H}_{1j}(n)\mathbf{X}_1(n) + \mathbf{H}_{2j}(n)\mathbf{X}_2(n) + \mathbf{W}_j(n), \quad j=1,2. \tag{7}$$

3 Adaptive Modulation in SFBC OFDM

3.1 Parallel Decomposition of the MIMO Channel Using SVD

Fig. 2 shows the equivalent model of MIMO OFDM. At the receiver, the *k*-th demodulated subcarrier vector in the *n*-th time slots is given by

$$\mathbf{R}(n,k) = \mathbf{h}(n,k)\mathbf{S}(n,k) + \mathbf{W}(n,k) \tag{8}$$

where $\mathbf{R}(n,k) = [R_1(n,k)\ R_2(n,k)]^T$ and the additive white Gaussian noise is $\mathbf{W}(n,k) = [W_1(n,k)\ W_2(n,k)]^T$. The channel matrix $\mathbf{h}(n,k)$ is as follows

$$\mathbf{h}(n,k) = \begin{bmatrix} H_{11}(n,k) & H_{21}(n,k) \\ H_{12}(n,k) & H_{22}(n,k) \end{bmatrix} \tag{9}$$

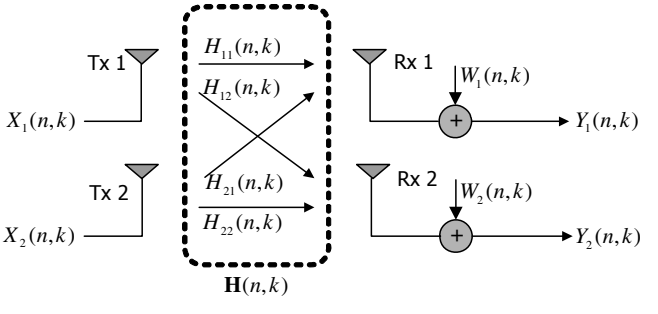


Fig. 2. An equivalent model of MIMO OFDM

We assume that both the transmitter and the receiver know $\mathbf{h}(n,k)$ at each instant. Let the instantaneous channel matrix have singular value decomposition

$$\mathbf{h}(n,k) = \mathbf{U}(n,k)\mathbf{\Lambda}(n,k)\mathbf{V}^H(n,k) \tag{10}$$

where $\mathbf{U}(n,k)$ and $\mathbf{V}(n,k)$ are unitary matrices, the matrix $\mathbf{V}^H(n,k)$ means the hermitian matrix of $\mathbf{V}(n,k)$ and $\mathbf{\Lambda}(n,k)$ is the diagonal matrix of singular values of $\mathbf{h}(n,k)$, i.e., $\mathbf{\Lambda}(n,k) = \text{diag}[\lambda_1(n)\ \lambda_2(n)]$ with $\lambda_1(n) \geq \lambda_2(n) \geq 0$. By transmit precoding($\bar{\mathbf{S}} = \mathbf{V}^H \mathbf{S}$) and receiver shaping($\bar{\mathbf{R}} = \mathbf{U}^H \mathbf{R}$) , the MIMO channel is transformed into parallel single input single output channels

$$\begin{aligned} \bar{\mathbf{R}}(n,k) &= \mathbf{U}^H(n,k)\mathbf{R}(n,k) \\ &= \mathbf{U}^H(n,k)\mathbf{h}(n,k)\bar{\mathbf{S}}(n,k) + \bar{\mathbf{W}}(n,k) \\ &= \mathbf{\Lambda}(n,k)\mathbf{S}(n,k) + \bar{\mathbf{W}}(n,k) \end{aligned} \tag{11}$$

where $\bar{\mathbf{W}} = \mathbf{U}^H \mathbf{W}$. Note that multiplication by a unitary matrix does not change the distribution of white Gaussain noise, that is, $\mathbf{W}$ and $\bar{\mathbf{W}}$ are identically distributed.

The SVD processing shown by Fig. 3 enables an MIMO OFDM system to adapt a suitable power/bit allocation to each subcarrier under constraints in a similar fashion of single input single output OFDM. However, in outdoor mobile environments, the MIMO channels can be quickly varied at each instant due to the mobility of mobile station. Therefore the SVD processing for the channel decomposition induces the burden complexity of the MIMO OFDM. But SFBC OFDM system turns the MIMO channel associated with each subcarrier into decoupled SISO channels without high complexity.

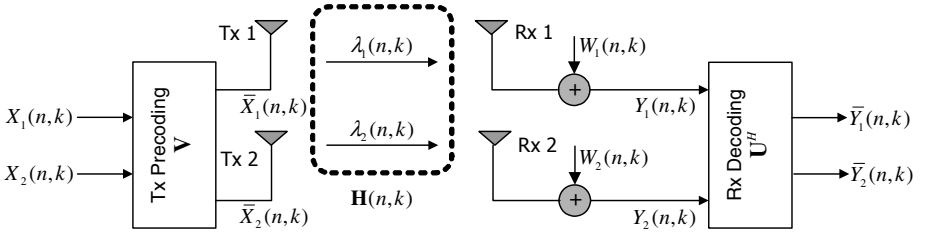


Fig. 3. An equivalent model of MIMO OFDM using SVD

3.2 Parallel Decomposition in SFBC OFDM

Equation (8) can be represented by the even and odd component vectors as follows

$$\begin{aligned} \mathbf{Y}_{j,e}(n) &= \mathbf{H}_{1j,e}(n)\mathbf{X}_{1,e}(n) + \mathbf{H}_{2j,e}(n)\mathbf{X}_{2,e}(n) + \mathbf{W}_{j,e}(n), \\ \mathbf{Y}_{j,o}(n) &= \mathbf{H}_{1j,o}(n)\mathbf{X}_{1,o}(n) + \mathbf{H}_{2j,o}(n)\mathbf{X}_{2,o}(n) + \mathbf{W}_{j,o}(n), \end{aligned} \quad j = 1,2. \tag{12}$$

This paper makes use of the following combining scheme at the receiver

$$\begin{aligned} \tilde{\mathbf{X}}_e(n) &= \mathbf{H}^*_{11,e}(n)\mathbf{Y}_{1,e}(n) + \mathbf{H}_{21,o}(n)\mathbf{Y}^*_{1,o}(n) + \mathbf{H}^*_{12,e}(n)\mathbf{Y}_{2,e}(n) + \mathbf{H}_{22,o}(n)\mathbf{Y}^*_{2,o}(n) \\ \tilde{\mathbf{X}}_o(n) &= \mathbf{H}^*_{21,e}(n)\mathbf{Y}_{1,e}(n) - \mathbf{H}_{11,o}(n)\mathbf{Y}^*_{1,o}(n) + \mathbf{H}^*_{22,e}(n)\mathbf{Y}_{2,e}(n) - \mathbf{H}_{12,o}(n)\mathbf{Y}^*_{2,o}(n). \end{aligned} \tag{13}$$

Assuming the frequency responses between adjacent subcarriers are approximately constant, i.e.,

$$\begin{aligned}
\mathbf{H}_{11,e}(n) &\approx \mathbf{H}_{11,o}(n) \\
\mathbf{H}_{12,e}(n) &\approx \mathbf{H}_{12,o}(n) \\
\mathbf{H}_{21,e}(n) &\approx \mathbf{H}_{21,o}(n) \\
\mathbf{H}_{22,e}(n) &\approx \mathbf{H}_{22,o}(n)
\end{aligned} \tag{14}$$

Finally, the combined signals can be rewritten by

$$\begin{aligned}
\tilde{\mathbf{X}}_e(n) &= \left(\left|\mathbf{H}_{11,e}(n)\right|^2 + \left|\mathbf{H}_{12,e}(n)\right|^2 + \left|\mathbf{H}_{21,e}(n)\right|^2 + \left|\mathbf{H}_{22,e}(n)\right|^2\right)\mathbf{X}_e(n) + \tilde{\mathbf{W}}_e(n) \\
\tilde{\mathbf{X}}_o(n) &= \left(\left|\mathbf{H}_{11,o}(n)\right|^2 + \left|\mathbf{H}_{12,o}(n)\right|^2 + \left|\mathbf{H}_{21,o}(n)\right|^2 + \left|\mathbf{H}_{22,o}(n)\right|^2\right)\mathbf{X}_o(n) + \tilde{\mathbf{W}}_o(n)
\end{aligned} \tag{15}$$

where

$$\begin{aligned}
\tilde{\mathbf{W}}_e(n) &= \mathbf{H}^*_{11,e}(n)\mathbf{W}_{1,e}(n) + \mathbf{H}_{21,o}(n)\mathbf{W}^*_{1,o}(n) + \mathbf{H}^*_{12,e}(n)\mathbf{W}_{2,e}(n) + \mathbf{H}_{22,o}(n)\mathbf{W}^*_{2,o}(n) \\
\tilde{\mathbf{W}}_o(n) &= \mathbf{H}^*_{21,e}(n)\mathbf{W}_{1,e}(n) - \mathbf{H}_{11,o}(n)\mathbf{W}^*_{1,o}(n) + \mathbf{H}^*_{22,e}(n)\mathbf{W}_{2,e}(n) - \mathbf{H}_{12,o}(n)\mathbf{W}^*_{2,o}(n).
\end{aligned} \tag{16}$$

The equation (15) which similar to equation (11) indicates that SFBC OFDM scheme turns the MIMO channel into decoupled SISO channels. This paper makes use of this equation for the adaptive modulation in MIMO OFDM.

3.3 Adaptive Bit Loading

In this paper, we consider the bit allocation scheme in [6]. We presuppose total transmit bits and load these bits onto each subcarrier in such a way that minimum energy is allocated to the entire transmission. Assume M-QAM is employed for each subcarrier, $b(n,k)$ bits per symbol are sent for the k-th subcarrier in the n-th OFDM symbol. According to [7][8], given the channel frequency response $H(n,k)$, the instantaneous bit error rate(BER) can be approximated by

$$P_e(n,k) = c_1 \exp\left\{-\frac{c_2 \dfrac{E_s}{N_0}\left|H(n,k)\right|^2}{2^{b(n,k)}-1}\right\} \tag{17}$$

where $c_1 = 0.2$, $c_2 = 1.6$, E_s is the symbol energy at the transmitter, N_0 is the variance of $\mathbf{W}(n)$. This paper chooses the allocation scheme to achieve the target BER ($P_r \le 10^{-2}$) as follows

$$b(n,k) = \log_2 \left[\frac{c_2 \frac{E_s}{N_0} \left| H(n,k) \right|^2}{\ln \frac{c_1}{P_r}} + 1 \right] \tag{18}$$

Let us consider the bit allocation in SFBC OFDM system. From the equation (15), the decoupled CSI for bit allocation is as follows

$$\left| \mathbf{H}(n,k) \right|^2 = \left| H_{11}(n,k) \right|^2 + \left| H_{12}(n,k) \right|^2 + \left| H_{21}(n,k) \right|^2 + \left| H_{22}(n,k) \right|^2 \tag{19}$$

By substituting $\left| \mathbf{H}(n,k) \right|^2$ into $\left| H(n,k) \right|^2$ in equation (18), the bit allocation for SFBC OFDM is performed and the next procedures for complete bit allocation are based on Chow's method. Note that the allocated number of bits between subcarriers is exactly identical, i.e., $b(n,k) = b(n,k+1)$, because the frequency responses between adjacent subcarriers are approximately constant.

4 Simulation Results

4.1 Simulation Parameters

The parameters of adaptive OFDM system are as follows. Carrier frequency is 2GHz and the channels bandwidth is 20MHz which is divided equally among 2048 tones. The channel is based on COST 207 for a hilly terrain area [9] and the SISO channels associated with different couples of transmit/receive antennas are statistically equivalent and independent. The RMS delay spread is 5μs. A guard interval of 22.6μs appended to each frame. A total of 4096 information bits transmitted in each OFDM frame, for an average 4 bits per subcarrier. Power allocation is uniformly performed. We assume that the total power from the two antennas for SFBC OFDM scheme is the same as the transmit power from the single transmit antenna. The velocities of mobile station are 60km/h and 100km/h, respectively. We allocate 0, 2, 4, or 6 bits to each subcarrier. So, each subcarrier is modulated using 4-, 16-, or 64-QAM, depending on the number of bits allocated. To compare with adaptive OFDM, the conventional OFDM scheme, called as an uniform OFDM, is uniformly modulated by 16-QAM. For the simulation according to feedback delay T_Δ, the minimum feedback delay is 81μs and the maximum delay is 810μs. For the purpose of the evaluation of various antenna schemes, three kinds of transmit(Tx)/ receive(Rx) antenna schemes are considered, i.e, 1Tx-1Rx, 2Tx-1Rx and 2Tx-2Rx, respectively.

4.2 Performance in Case of Perfect CSI

The perfect CSI for bit allocation can be referred as there is no feedback delay. It means very slow fading environment. Accordingly, the performance results show the evaluation of the efficiency of adaptive modulation scheme. Firstly, Fig. 4 shows the

performance of uniform OFDM according to various Tx/Rx antenna schemes. In comparison with 1Tx-1Rx antenna scheme, the power gain for 2Tx-1Rx antenna schemes at a BER of 10^{-3} is about 8 dB. In case of 2Tx-2Rx scheme, the power gain at a BER of 10^{-3} is about 15dB. These results explain that a considerable diversity gain can be obtained when uniform OFDM system employs a diversity scheme. Now, from Fig. 5, we can observe the power gain of adaptive OFDM system employing a diversity scheme. The power gain for 2Tx-1Rx antenna scheme at a BER of 10^{-3} is about 1.5 dB. In case of 2Tx-2Rx scheme, the power gain is about 5dB. From this result, the diversity gains in adaptive modulation are much less than those of uniform modulation. That is the reason why the adaptive modulation does very well deal with frequency-selectivity itself .

4.3 Effect of the Outdated CSI in Mobile Situation

Let us now shift the emphasis away from the perfect CSI to the outdated CSI. This raises the question of how the performance of adaptive OFDM system with diversity scheme appears in mobile fading environments. Fig. 6 indicates that the feedback delay has an effect on the performance of adaptive SFBC OFDM with 2Tx/1Rx antenna scheme. As expected, the BER is gradually degraded as the feedback delay increases. This performance degradation is due to unavailability of CSI at the transmission time. In mobile situation, the CSI at the transmission instant is already the outdated information because the channel impulse response is time-varying. Let us examine that an adaptive OFDM system employing space-frequency block coding scheme is one of ways how to overcome the effects of feedback delay. As mentioned above, for the purpose of the evaluation the performance according to feedback delay, various simulations in terms of feedback delay are performed when the velocities are 60km/h and 100km/h respectively. To begin with, Fig. 7 indicates the simulation result when the feedback delay is 324μs and 810μs, respectively. Allowing for a BER of 10^{-3}, let us compare the required power in Fig. 5 with that in Fig. 7. In case of 1Tx-1Rx, let us compare with the perfect CSI of Fig. 5. An adaptive OFDM system with feedback delay needs the additional power more than about 8 dB. It is shown that there is no merit of adaptive 1Tx-1Rx OFDM when feedback delay is long. On the other hand, in case of 2Tx-1Rx scheme, adaptive SFBC OFDM system with feedback delay needs the additional power of about 2dB and 5dB, respectively. We can see that adaptive OFDM system employing a diversity scheme mitigates the effect of feedback delay. Also, adaptive SFBC OFDM system with 2Tx-2Rx scheme requires more than only 1dB. From this result, the performance degradation of adaptive OFDM due to the outdated CSI can be mitigated by diversity technique and we can refer the adaptive 2Tx-2Rx SFBC OFDM as an excellent system which have scarcely power loss in spite of severe feedback delay. Finally, let us see the performance according to the feedback delay. Fig. 8 indicates the performances of adaptive OFDM system along diversity scheme when the feedback delay is from 81μs to the maximum 810μs. SNR is 25dB and the

respective velocities are 60km/h and 100km/h. Apparently we can see that the performance of adaptive OFDM with diversity schemes is much better than that of adaptive SISO OFDM.

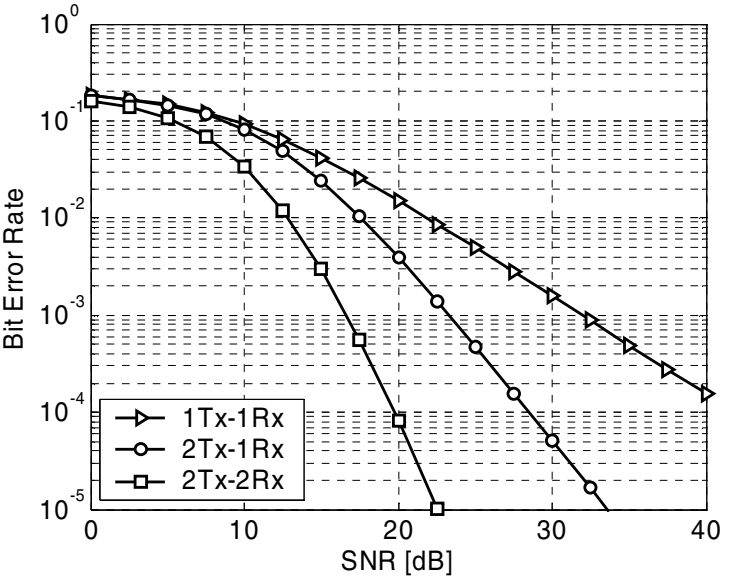


Fig. 4. BER curves of uniform OFDM according to Tx and Rx antenna schemes

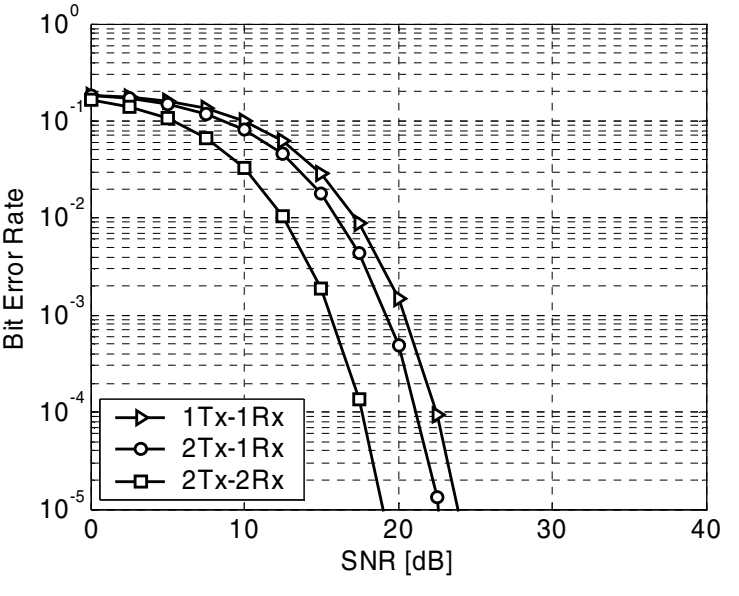


Fig. 5. BER curves of adaptive OFDM according to Tx and Rx antenna schemes

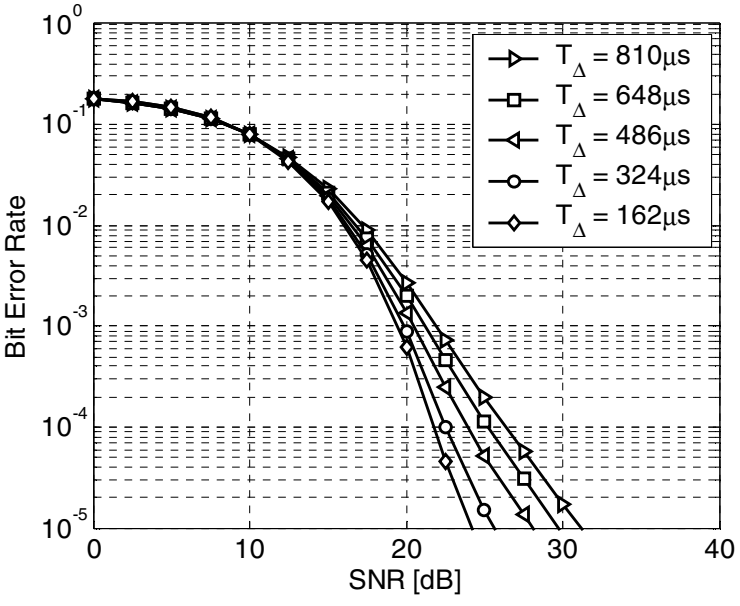


Fig. 6. BER curves according to feedback delay

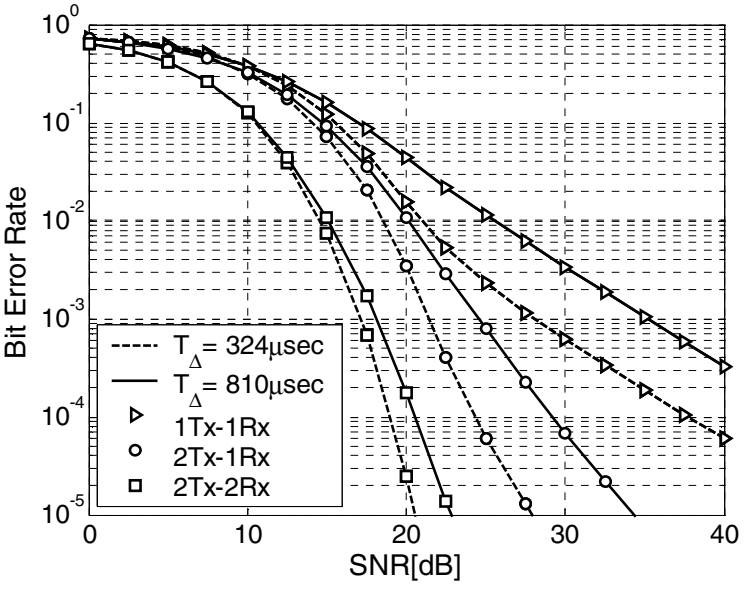


Fig. 7. BER curves according to diversity scheme in case that feedback delays are 324μs and 810μs respectively

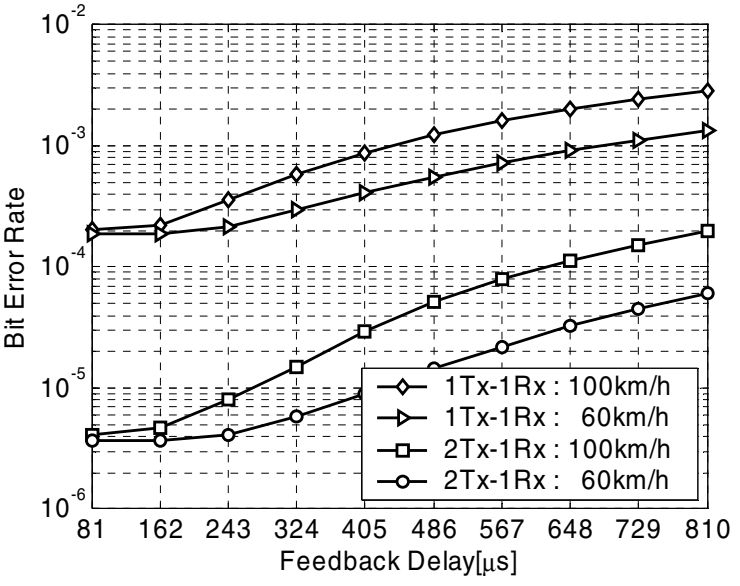


Fig. 8. BER curves according to feedback delay & Tx/Rx antenna schemes.(25 dB)

5 Conclusions

In this paper combining an adaptive bit allocation scheme with SFBC OFDM system has been discussed. It has been illustrated that the CSI from SVD of MIMO channel is identical to the CSI from SFBC OFDM. From the various simulations, the performance of adaptive SFBC OFDM has been evaluated. Particularly, the BER performance according to the feedback delay has been indicated in detail. In the results, it is very interesting that the diversity schemes mitigate the effect of long feedback delay for adaptive OFDM. Most of all, adaptive SFBC OFDM with 2Tx-2Rx antenna scheme has made an excellent performance in spite of a severe feedback delay.

References

1. T. Keller and L. Hanzo, "Adaptive multicarrier modulation: a convenient framework for time-frequency processing in wireless communications," *Proc. Of the IEEE*, vol. 88, pp. 611-640, May 2000.
2. S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J, Select. Areas Comm.*, vol. 16, pp. 1451-1458, Oct. 1998.
3. K. F. Lee and D. B. Williams, "A space-time coded transmitter diversity technique for frequency selective fading channels," *in Proc. of the 2000 IEEE, SAMSP workshop*, pp. 149-152.
4. H. Bolcskei and A. Paulraj, "Space-frequency coded broadband OFDM systems," *in Proc. Of Wireless Comm. Networking Conf.*, pp. 1-6. Sept. 2000.

5. Z. Liu, Y. Xin and G. B. Giannakis, "Space-time-frequency coded OFDM over frequency-selective fading channels," *IEEE Trans. Sig. Proc*., vol. 50, pp. 2465-2476, Oct. 2002.
6. P. S. Chow, J. M. Cioffi and J. A. C. Bingham, "A practical discrete multi-ton transceiver allocation algorithm for data transmission over spectrally shaped channels," *IEEE Trans. on Comm*, vol. 43, pp. 773-775, Apr 1995.
7. S. T. Chung and A. J. Goldsmith, "Degrees of freedom in adaptive modulation: a unified view," *IEEE trans. On Comm*., vol. 49, pp. 1561-1571, sep. 2001
8. S. Ye, R. S. Blum and L. L. Cimini, "Adaptive modulation for variable-rate OFDM systems with imperfect channel information," *Proc, VTC 2002*, pp. 767-771.
9. M. Patzold, *Mobile Fading Channels*, Wiley, 2002.

Generalized Rake Receiver for Spreading-IFDMA Systems

Wei Wang[1], Ling Wang[2], Zhiqiang He[1], Jiaru Lin[1], Wei Qiu[2], and Elena Costa[3]

[1] School of Information Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, P.R. China
sethvivid@163.com, hezq@bupt.edu.cn, jrlin@public.bta.net.cn
[2] Siemens Ltd., China, Corporate Technology, Radio Technology and Solution, Beijing 100102, P.R. China
{wangling, wei.qiu}@siemens.com
[3] Siemens AG, Com MN PG NT RI 4, Munich D-81541, Germany
elena.costa@siemens.com

Abstract. Spreading-Interleaved Frequency Division Multiple Access (IFDMA) providing code domain multiplexing for one IFDMA channel shows improved spectrum efficiency and good compatibility with CDMA systems while maintaining advantages of IFDMA systems. A generalized Rake receiver for Spreading-IFDMA is proposed in this paper, which combines jointly de-repetition, equalization, and de-spreading processing. Similar to the conventional CDMA systems, the guard interval in Spreading-IFDMA symbols is not necessary, which means that spectrum efficiency can be further improved over IFDMA systems. With digital simulations and performance analysis, the proposed generalized Rake receiver demonstrates better BER performance, robustness, and lower computational complexity.

1 Introduction

Interleaved Frequency Division Multiple Access (IFDMA) has been proposed as a promising multiple access technique especially for future uplink transmission [1][2] since it provides several advantages such as low Peak-to-Average Power Ratio (PAPR), high flexibility and granularity for bandwidth adjustment, and good frequency diversity performance [3]. In recent 3GPP Long Term Evaluation (LTE) study item, the single carrier FDMA scheme has been chosen as the uplink multiple access technique for FDD/TDD modes, where it is preferred to exploit distributed FDMA for contention-based data or signaling transmission [4]. IFDMA in time domain implementation of distributed FDMA has attracted much more discussion and performance evaluation during 3GPP LTE [5]. In IFDMA systems, compression and periodic repetition of a given data vector are used to generate the transmitted signal with equally spaced distribution of frequency components with zero-points in-between where frequency components of other users can be positioned. Its comp-shaped frequency spectrum resembles that of multi-carrier systems, but IFDMA exhibits the same low PAPR as single carrier systems. For accurate positioning of

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 425 – 436, 2006.

different user signals the compressed and repeated data vector is shifted in frequency domain by a user specific phase factor. Hence, IFDMA signal can also obtained by choosing the Discrete Fourier Transform (DFT) as precoding of an OFDMA signal [3][6].

Variable spreading and chip repetition factors (VSCRF)-CDMA is proposed as a broadband wireless access scheme for uplink transmission [7], which adaptively changes the spreading and chip repetition factors in accordance with the cell structure, the number of simultaneous accessing users and the propagation channel conditions. In the isolated-cell environment considered in VSCRF-CDMA, the principle of symbol repetition in IFDMA is applied to the chip sequence after time domain spreading.

Actually, the combination of IFDMA and time domain spreading can also be used in uplink transmission in multi-cell environment. In this paper, we name this combination as Spreading-IFDMA for convenience. The pilot signal multiplexing in code domain for multiple uplink users is a main candidate in current 3GPP LTE discussion since it is straightforward to obtain the channel state information of the whole transmission bandwidth for further channel-dependent scheduling [4]. On the other hand, Spreading-IFDMA systems show inherent backward compatibility with CDMA systems.

However, current consideration for Spreading-IFDMA has to insert guard interval e.g. cyclic prefix (CP), to achieve good demodulation performance. Although the insertion of guard interval avoids the inter-block interference, it reduces the spectrum efficiency. The improvement of spectrum efficiency will be one of the most important targets in future radio systems. In this paper, the generalized RAKE receiver for Spreading-IFDMA is proposed, which shows considerable performance merits while reducing greatly the complexity of time domain equalization. Furthermore, similar to traditional CDMA systems, it is not necessary to insert guard interval any more, which leads to the improvement of spectrum efficiency over pure IFDMA systems.

The rest of this paper is organized as follows. In section 0, the system framework, signal model, and typical receiver structure of Spreading-IFDMA are introduced. In section 0, the generalized Rake receiver for Spreading-IFDMA systems without guard interval is proposed and orthogonality proof is also provided in multiple users scenario. Digital simulation results and performance evaluation for the proposed receiver with emphasis on robustness are demonstrated in Section 0. Finally, some conclusions are given in Section 0.

2 System Framework and Signal Model

The system framework of Spreading-IFDMA with conventional receiver [7], i.e. concatenated processing for equalization and de-spreading (CPEDS), is shown in **Fig. 1**, where it is flexible to distinguish different users or physical channels in frequency or code domain in Spreading-IFDMA systems.

It is assumed that B is the number of modulated symbols contained in each block and the corresponding block duration is T_s. $Q=G\cdot B$ is the number of chips in each block, where G denotes the spreading gain. A block of chips after spreading can be described by

$$\mathbf{d}^k = \left[d_0^k, d_1^k, ..., d_{Q-1}^k \right]^T = \begin{bmatrix} \mathbf{s} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{s} & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{s} \end{bmatrix} \cdot \begin{bmatrix} b_0^k \\ b_1^k \\ \vdots \\ b_{B-1}^k \end{bmatrix} \tag{1}$$

where $\mathbf{d}^k$ denotes the spread chips vector by Q×1 and b_i^k is the ith modulated symbol for user k. $\mathbf{s}$ is the spreading code vector by G×1, where all users are allocated the same spreading code for convenience. However, it is straightforward to multiplex different users or physical channels in code domain.

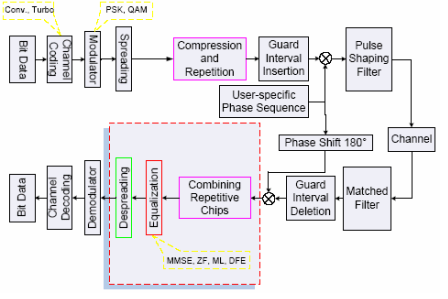


Fig. 1. System framework with CPEDS

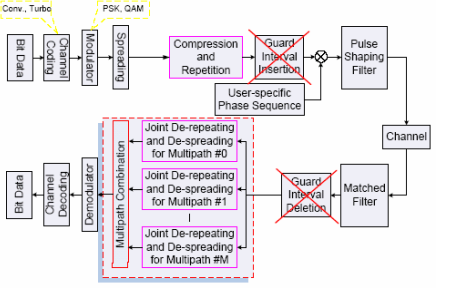


Fig. 2. System framework without guard interval

By compressing each of the Q chips with chip duration T_{cb} and repeating the resulting compressed block (L+L_Δ)-times, a Spreading-IFDMA block $\mathbf{c}^k$ can be obtained

$$\mathbf{c}^k = \frac{1}{L+L_\Delta} \underbrace{\left[d_0^k, d_1^k, \cdots, d_{Q-1}^k, \cdots, d_0^k, d_1^k, \cdots, d_{Q-1}^k \right]^T}_{(L+L_\Delta)-times} \tag{2}$$

where the tiny chip duration T_{ca} after compression is determined by

$$T_{ca} = T_{cb} / \left(L + L_\Delta \right) = T_s / \left(G \left(L + L_\Delta \right) \right) \tag{3}$$

The first QL_Δ tiny chips belong to the guard interval and the guard duration equals to

$$T_\Delta = L_\Delta \cdot Q \cdot T_{ca} \tag{4}$$

where L_Δ should be chosen by the following condition if equalizers are exploited

$$T_\Delta > \tau_{\max} \tag{5}$$

where $\tau_{\max}$ is the maximum delay of the transmission channel. Furthermore, the transmission signal $\mathbf{x}^k$ is constructed by element-wise multiplication of the Spreading-IFDMA symbol $\mathbf{c}^k$ with the following user-specific phase vector.

$$\mathbf{p}^k = \left[1, \exp\left(-\mathrm{j}\Phi^k\right), \cdots, \exp\left(-\mathrm{j}\cdot n\cdot\Phi^k\right), \cdots, \exp\left(-\mathrm{j}\cdot\left(QL_c-1\right)\cdot\Phi^k\right)\right]^T \tag{6}$$

where $L_c = L + L_\Delta$ and user-specific phase Φ^k is chosen to be

$$\Phi^k = \left(k2\pi\right)/\left(QL\right) \tag{7}$$

By assigning to each user a different set of orthogonal frequencies, the multiple access schemes can be obtained. The resulting transmission signal vector $\mathbf{x}^k$ can be written as

$$\mathbf{x}^k = \left[c_0^k, c_1^k \exp\left(-\mathrm{j}\Phi^k\right), \cdots, c_n^k \exp\left(-\mathrm{j}\cdot n\cdot\Phi^k\right), \cdots, c_{(QL_c-1)}^k \exp\left(-\mathrm{j}\cdot\left(QL_c-1\right)\cdot\Phi^k\right)\right]^T \tag{8}$$

After transmission over an arbitrary channel with impulse response vector $\mathbf{h}^k = \left[h_0^k, h_1^k, \cdots, h_M^k\right]^T$ of dimension (M+1) and additional additive white Gaussian noise (AWGN) distortion, the nth received component corresponding to user k , y_n^k , can be written by

$$y_n^k = \sum_{m=0}^{M} x_{n-m}^k h_m^k \ , \ n = 0, \cdots, QL_c + M - 1 \tag{9}$$

In the multiuser system with K active users, the received vector by (QL_c+M) is

$$\mathbf{y} = \sum_{k=1}^{K} \mathbf{y}^k = \sum_{k=1}^{K} \mathbf{H}^k \cdot \mathbf{x}^k + \mathbf{z} \tag{10}$$

where $\mathbf{H}^k$ is the convolution matrix of the channel by (QL_c+M)×QL_c and one-sided noise spectral density of AWGN distortion vector $\mathbf{z}$ with dimension of (QL_c+M) is N_0. The nth component y_n becomes

$$y_n = \sum_{k=1}^{K} \sum_{m=0}^{M} x_{n-m}^k h_m^k + z_n \tag{11}$$

In CPEDS based receiver [7] shown in **Fig. 1**, the received data chips are combined in the de-repetition module first and then enter the equalizer to resist the ISI. The equalized data chips are further combined by using the de-spreading module. Therefore, equalization and de-spreading processing are implemented independently. Some popular equalizers can be used, but there exists high computational complexity due to its chip level implementation.

3 Generalized Rake Receiver for Spreading-IFDMA Without Guard Interval

The appropriate combination of resolvable multipath components of the radio channel by a Rake receiver in traditional CDMA systems can considerably improve the performance. In Spreading-IFDMA systems, multiple access users can be distinguished by means of not only their distinct user-specific code sequences but also

the user-specific phase sequences. Hence, .it is crucial to guarantee the orthogonality between different users in frequency domain in receivers of Spreading-IFDMA systems. In this section, the generalized Rake receiver for Spreading-IFDMA systems without guard interval, i.e. L_Δ=0, is introduced and its corresponding block diagram is shown in **Fig. 2**.

Spread spectrum systems are not only resistant to multipath fading, but they can also exploit the multipath components to improve the performance of the system. Based on the fact that the multipath components are practically uncorrelated from one another when their relative propagation delays exceed a tiny chip period and PN sequences are exploited, Rake receiver consisting of a bank of correlators, each of which is corresponding to a particular multipath component of the desired signal, can exploit the multipath components to improve the performance of the system. Furthermore, outputs of the correlators are weighted according to certain optimization criterions to generate the enhanced signal estimation, e.g. maximum signal-noise-plus-interference ratio, maximum likelihood, and minimum mean square error (MMSE). Similar to traditional CDMA systems, the guard interval for Spreading-IFDMA systems in **Fig. 1** is discarded due to the multipath combination capability of the generalized Rake receiver shown in **Fig. 2**, which means the improvement of spectrum efficiency.

3.1 Joint Processing for De-repetition and De-spreading in a Singer Finger

During de-repetition and de-spreading, only tiny chips within [0, $QL+M$-1] will be exploited. For simplicity, noise free transmission is assumed. Therefore, the joint de-repetition and de-spreading in time dispersive channels corresponding to the first path can be derived as follows.

$$r_i^k = \sum_{l=0}^{L-1}\sum_{g=0}^{G-1} y_{lQ+iG+g} \cdot s_g \cdot e^{\mathrm{j}(lQ+iG+g)\Phi^k} \tag{12}$$

$$= \sum_{j=1}^{K}\sum_{m=0}^{M}\sum_{l=0}^{L-1}\sum_{g=0}^{G-1} c^j_{lQ+iG+g-m} \cdot h_m^j \cdot s_g \cdot e^{\mathrm{j}m\Phi^j} \cdot e^{\mathrm{j}(lQ+iG+g)\left(\Phi^k-\Phi^j\right)} \tag{13}$$

$$= \begin{cases} \sum_{m=0}^{M} h_m^k \cdot e^{\mathrm{j}m\Phi^k} \sum_{g=0}^{G-1} b^k_{\left\lfloor\left[(iG+g-m)\bmod Q\right]/G\right\rfloor} \cdot s_{\left[(iG+g-m)\bmod Q\right]\bmod G} \cdot s_g, & if\ \ j=k \\ 0, \quad otherwise \end{cases} \tag{14}$$

The equations above show that the orthogonality between distinct users at the receiver is maintained even in a time-dispersive channel if $K \le L$. There is no MAI within a single cell of a cellular mobile ratio communications system. Furthermore, this statement applies for both the uplink and the downlink transmission since equations (**13**) and (**14**) holds for both links. Moreover, this statement is also valid for time-variant channels, but only if the channel impulse response can be assumed to be time-invariant within the duration of T_s. The degradation due to fast time-variant channels depends on the time-variance of the transmission channel.

The Spreading-IFDMA system is a typical wideband signal transmission since the tiny chip rate $1/T_{ca}$ after compressing and repeating is typically much larger than the flat fading bandwidth of the channel. Pseudo-Noise (PN) sequences with very low autocorrelation and correlation properties are usually chosen as the spreading sequences. If multipath components are delayed in time by more than a tiny chip duration, they appear like uncorrelated noise which is ignored by the receiver. Therefore, the spread-spectrum operation can effectively alleviate the multipath interference and multiple access interference from different code channels by virtue of its code-correlation receiver. For user k Equation (**14**) can be further written as

$$r_i^k \approx h_0^k b_i^k \tag{15}$$

The estimated transmitted symbol $\hat{b}_i^k$ can be obtained by channel matching or single-tap equalizing.

$$\hat{b}_i^k = \left(h_0^k\right)^* r_i^k \approx \left|h_0^k\right|^2 b_i^k \tag{16}$$

Although code domain multiplexing in Spreading-IFDMA with correlation processing provides more flexibility than pure IFDMA systems, it induces interference between code channels simultaneously allocated to the same frequency channels due to multipath propagation. That's why the strict equality does not appear in Equation (**15**) and (**16**). Fortunately, choice of code sequences with very low autocorrelation and correlation properties, synchronization in IFDMA, and multiuser detection techniques can resist these interferences. Only single path information above is exploited. The performance of the receiver will be improved when multipath components are combined in some effective ways.

3.2 Rake Multipath Combination

The relative amplitudes and phases of the multipath components are found by correlating the received waveform with delayed versions of the signal or vice versa. Usually, the P strongest multipath components are chosen as the fingers of Rake receiver. Here, we assume that the p-th finger is corresponding to the multipath component with delay pT_{ca}, where p=0, 1, … , P-1. According to Equation (**14**), the output of the pth finger of Rake receiver by exploiting the joint de-repetition and de-spreading can be written as

$$r_{ip}^k = \sum_{l=0}^{L-1} \sum_{g=0}^{G-1} y_{lQ+iG+g} \cdot s_{(g-p) \bmod G} \cdot e^{\mathrm{j}(lQ+iG+g-p)\Phi^k} \tag{17}$$

$$\begin{cases} \approx h_p^k b_i^k, if \ \ j=k, p=m \\ = 0, other \end{cases} \tag{18}$$

The output signal-to-interference-plus-noise ratio of the Rake receiver can be improved significantly by proper combination of the P single fingers outputs. The output of Rake receiver is

$$r_i^k = \sum_{p=0}^{P-1} \beta_p \cdot r_{ip}^k \tag{19}$$

There are many possible multipath combination methods, e.g. coherent combination, maximum ratio combination, equal gain combination etc. Here, popular coherent and noncoherent combination techniques are considered. In coherent combination, channel information is required, which can be obtained by means of different channel estimation methods. In this case, the weighting coefficients are given by

$$\beta_p = \left(\hat{h}_p^k\right)^* \tag{20}$$

where $\hat{h}_p^k$ is the estimated channel fading coefficient of the p-th path of user k. In non-coherent combination, the weighting coefficients are determined by

$$\beta_p = \left(r_{ip}^k\right)^2 \Big/ \sum_{p=0}^{P-1} \left(r_{ip}^k\right)^2 \tag{21}$$

3.3 Implementation Illustration

Here, we assume spreading gain G=2, repetition factor L=3, number of modulated data symbols contained in an IFDMA block equal to B=2, and the number of fingers in the Rake receiver M+1. Implementation steps are summarized as follows.

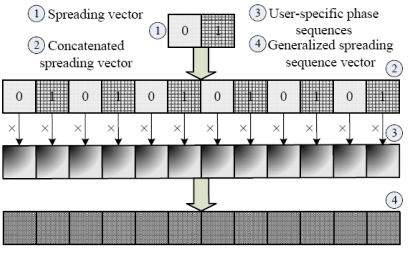


Fig. 3. Generalized spreading sequences

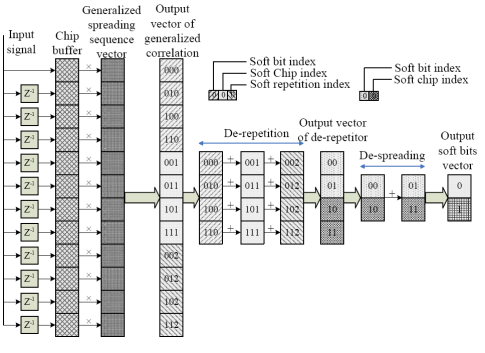


Fig. 4. Processing procedure for a single finger

Step 1. Construction of generalized spreading sequences

(i) To construct the concatenated spreading vector with dimension of GBL×1 according to $\mathbf{g}=[\mathbf{s}^T, \mathbf{s}^T, \ldots, \mathbf{s}^T]^T$; (ii) To construct the generalized spreading sequence vector, which is equal to the elementwise product of the user-specific phase sequence vector by the concatenated spreading vector, i.e. $\mathbf{e}=\mathbf{g}\bullet\mathbf{p}$ and shown in **Fig. 3**.

Step 2. Generalized correlation

(i) To assemble a received chip vector with the same dimension as the generalized spreading sequence vector corresponding to a delayed multipath vector; (ii) To

correlate the assembled received vector by using the elementwise product of the received chip vector by the generalized spreading vector.

Step 3. De-repetition processing
(i) To segment the output vector of the generalized correlation into L subvectors with dimension of $(GB)\times1$; (ii) To sum up the L subvectors to form a output vector with the dimension of $(GB)\times1$

Step 4. De-spreading processing
(i) To Segment the output vector of the de-repetition processing into B subvectors, each of which has the dimension of $G\times1$; (ii) To respectively sum up the elements of each vector of B subvectors and then obtain B outputs; (iii) To assemble B outputs into the new vector with the dimension of $B\times1$.
Step 2 to Step 4 are shown in **Fig. 4**.

Step 5. Multiple fingers combination
(i) To save the vector after de-spreading processing in a buffer; (ii) To repeat Step 2 to Step 4 until to get $M+1$ vectors corresponding to $M+1$ different multipath version; (iii) To combine the P vectors selected from $M+1$ vectors according to some criteria.

Table 1. System simulation parameters

Items	Value	Items	Value
System bandwidth	2.5 MHz	Channel model	COST 207 'TU'
Repetition times	10	Modulation scheme	QPSK
Spreading codes	Gold, 7	Num. of users	10
Num. of repetitive modulated symbols	2	Num. of chips to be repeated	2×7
Rake combination scheme	Maximum ratio combination	Frame length	4.48 ms (No CP) 5.04 ms (CP)
Num. of Rake fingers	6	CPEDS	MMSE based

4 Digital Simulation and Performance Evaluation

Digital simulation and performance evaluation of the proposed generalized Rake receiver in Spreading-IFDMA systems are given with emphasis on robustness on frequency offset, timing error, and channel estimation error. Performance comparisons with CPEDS receiver for Spreading-IFDMA with cyclic prefix are provided to show the improved detection performance and spectrum efficiency. The "Typical Urban area" (TU) scenario of Cost 207 channel model is adopted in all simulations. To demonstrate the inherent performance of the multiple access scheme of Spreading-IFDMA, the error-correct codes are not considered in simulations. The link level simulation chain of Spreading-IFDMA systems is set up on the MLDesigner environment in Linux OS. System simulation parameters used in this paper are shown in **Table 1**.

4.1 Influence of Frequency Offset

Usually, frequency offset is induced by Doppler shift, inaccurate oscillator, or phase noise. In Spreading-IFDMA systems, the user-specific phase is set according to Equation (7) and the equivalent normalized carrier frequency of user k is $f_{norm}^{k} = k/(QL)$. The normalized carrier frequency spacing between two adjacent users equals to $\Delta f_{\text{norm}}=1/(QL)$. In this experiment, the Bit Error Rate (BER) performance of generalized Rake receiver of Spreading-IFDMA without guard interval is simulated, where the normalized frequency offset is set by 0, 0.1786e-3, 0.2381e-3, 0.3571e-3, and 0.7143e-3. The corresponding absolute frequency offset is 0, 0.4462, 0.5952, 0.8929, and 1.7857 KHz, respectively. From the simulation results shown in **Fig. 5**, it can be inferred that Spreading-IFDMA systems without guard interval have good robustness against frequency offset under these simulation conditions. For example, BER performance declines just about 1dB at 10e-3 level, when frequency offset reaches 1/30 of Δf_{norm}, i.e. 595.2Hz. However, for restricting performance degradation for frequency offset in much less scale, it is necessary to add the frequency spacing between users.

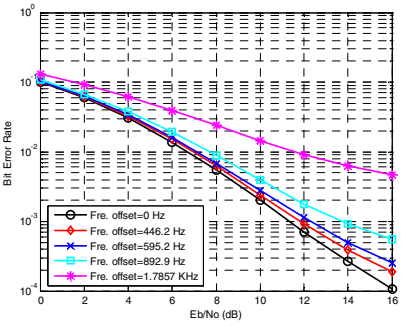


Fig. 5. BER versus E_b/N_0 with frequency offset

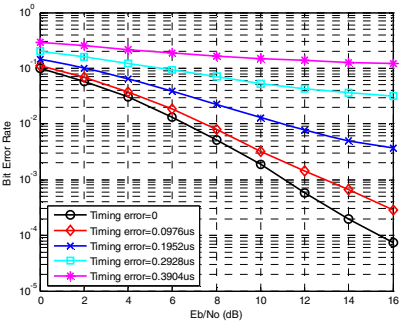


Fig. 6. BER versus E_b/N_0 with timing error

4.2 Influence of Timing Error

Here, RRC pulse-shaping filter with roll-off α=0.22 as recommended by 3GPP is used. Therefore, the tiny chip duration corresponding 2 MHz bandwidth equals to

$$T_{sc} = (1+\alpha)/B_{sys} = 0.488\,us \tag{22}$$

In **Fig. 6**, the robustness performance of the proposed receiver upon timing error is simulated, where the timing error is, 0, 0.0976, 0.1952, 0.02928, 0.3904 us, respectively. From this figure, it can be seen that the performance degradation at 10e-3 with timing error of $T_{\text{sc}}/5$, i.e. 0.0976 us, is approximately 2dB. It is clear that the performance of the receiver will be improved by increasing the accuracy of frame and symbol synchronization. On uplink scenario, large timing error will also induce multiple access interference in Spreading-IFDMA systems. However, by adding

appropriate guard interval to the head of each frame to put up with frame synchronization error, multiple access interference is expected to be reduced.

4.3 Influence of Number of Active Users

In spreading-IFDMA systems, different users or physical channels can be specified by different spreading sequence or phase parameters. The combination of the two allocation methods can afford more active users and **Fig. 7** shows the corresponding BER performance with 10, 15, and 20 active users on the condition of parameters in **Table 1**. In this case, the BER performance will be decreased with the increasing of number of active users since not all multiple users are orthogonal each other on frequency domain. Similar to the CDMA system, the link performance can be improved by choosing better spreading sequences or exploiting advanced multiple users detection methods. **Fig. 8** shows the relevant performance when setting the repetition time be 20, where different active users are allocated specific phase and the same spreading sequence. In this case, the performance almost keeps the same with the increasing of number of active users since the system become orthogonal on frequency domain.

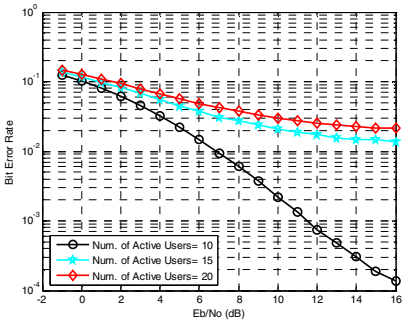


Fig. 7. BER with varying num. of users, case 1

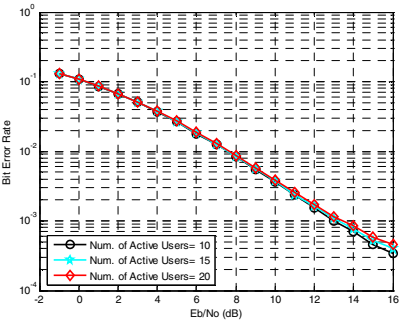


Fig. 8. BER with varying num. of users, case 2

4.4 Influence of Channel Estimation Error

In the simulation experiments above, we suppose that the Channel State Information (CSI) at the receiver is perfect. However, any channel estimation methods will induce error more or less in an actual system. The error vector of channel state information (CSI) can be calculated by $\mathbf{e}_k = \hat{\mathbf{h}}_k - \mathbf{h}_k$, where $\mathbf{h}_k$ is the actual channel response vector while $\hat{\mathbf{h}}_k$ is its estimated vector. Furthermore, the relative error of the CSI is defined as $\gamma = \|\mathbf{e}_k\| / \|\mathbf{h}_k\|$.

In this digital simulation, the robustness on channel estimation error of generalized Rake receiver in Spreading-IFDMA is evaluated, shown in **Fig. 9**, where the relative channel estimation error (RCEE) is 0, 10%, 30%, and 50%, respectively.

From this figure, we can see that when relative channel estimation error is lower than 10%, there is almost little influence on the Rake receiver of the Spreading-IFDMA

without guard interval. The BER performance degradation is less than about 1*dB* on the 10^{-3} level if the relative channel estimation error is not over 30%. Therefore, the receiver has strong robustness against channel estimation error.

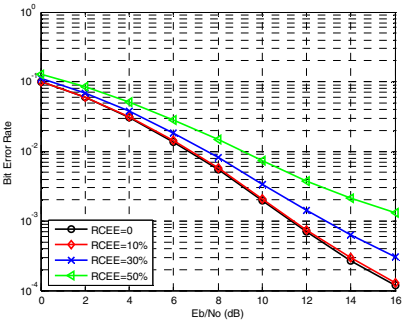


Fig. 9. BER versus Eb/N0 with CSI error

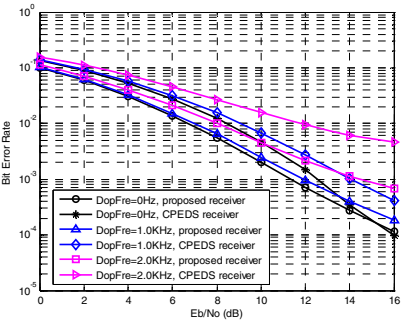


Fig. 10. BER performance comparison

4.5 Performance Comparison Between Generalized Rake Receivers and CPEDS

In this section, we give simulation results of the proposed Rake receiver with different Doppler shift in Spreading-IFDMA system framework without guard interval in comparison with Minimum Mean Square Error (MMSE) based CPEDS receiver in the conventional systems structure with guard interval.

From **Fig. 10**, it can be seen that the BER performance of the proposed Rake receiver in the Spreading-IFDMA system framework is more robust against maximum Doppler shift than that of the CPEDS receiver in the conventional Spreading-IFDMA structure because of its shorter symbol structure due to the removal of guard interval. For low E_b/N_0, e.g. from 0 to 15 dB, the BER performance of the proposed Rake receiver in the Spreading-IFDMA system framework is better than that of the CPEDS receiver in the conventional Spreading-IFDMA structure since the proposed Rake receiver matches the channel much better, while the BER performance of the latter will exceed that of the proposed Rake receiver on the condition of high E_b/N_0 because the inter-symbol interference becomes dominant, e.g. when E_b/N_0 is equal to 16 and maximum Doppler shift is equal to zero. Furthermore, the Spreading-IFDMA system without guard interval can improve the spectrum efficiency 12.5% to that with guard interval. On the other hand, MMSE based CPEDS receiver requires complex multiplication of $(19(GB)^3/6)+(GB)^2+4GB$ while the generalized Rake receiver only needs complex multiplication of $GBL(M+1)+MB$. Thus, the proposed receiver reduces computational complexity about 51% over the CPEDS receiver in presented simulation environment.

5 Conclusions

Generalized Rake receiver by using multipath components information combines jointly de-repetition, equalization, and de-spreading processing for Spreading-IFDMA

systems. Similar to the CDMA systems, guard interval in transmitted symbols of Spreading-IFDMA with the proposed receiver is not necessary and hence the frequency spectrum efficiency can further be improved. By using Rake combination methods for multiple fingers, the proposed generalized Rake receiver demonstrates better BER performance, robustness, and lower computational complexity.

Acknowledgment

This work has been performed in the framework of the Joint Research on Beyond 3G (JRB3G) project funded by Siemens AG and Siemens Ltd. China. The authors would like to acknowledge the contribution of their colleagues.

References

1. Sorger, U., Broeck, I. D., Schnell, M.: Interleaved FDMA – A new spread-spectrum multiple-access scheme. Conference Proceedings of the IEEE International Conference on Communications, Atlanta (1998) 1013–1017
2. Schnell, M., Broeck, I. D.: Application of IFDMA to mobile radio transmission. Conference proceedings of the IEEE International Conference on Universal Personal Communications, Florence (1998) 1267–1272
3. Frank, T., Klein, A., Costa, E.: Interleaved orthogonal frequency division multiple access with variable data rates. International OFDMA-workshop, Hamburg (2005)
4. 3GPP : Physical layer aspects for evolved UTRA (Release 7), TR 25.814, V1.2.3 (2006)
5. Motorola: Simulation Methodology for EUTRA UL: IFDMA and DFT-Spread-OFDMA. 3GPP RAN1 #43 R1-051335, Seoul (2005) 7–11
6. Dinis, R., Falconer, D., Chan, T., L., Sabbaghian, M.,: A multiple access scheme for the uplink of broadband wireless systems. in Proc. GLOBECOM'04, vol. 6. Dallas (2004) 3808–3812
7. Goto, Y., Kawamura, T., Atarashi, H., Sawahashi, M.: Variable spreading and chip repetition factors (VSCRF)-CDMA in reverse link for broadband wireless access. 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, Beijing (2003)

A Key Management Scheme for Large Scale Distributed Sensor Networks

Yong Ho Kim*, Hwaseong Lee, Dong Hoon Lee, and Jongin Lim

Center for Information Security Technologies (CIST),
Korea University, Seoul, Korea
{optim, hwaseong, donghlee, jilim}@korea.ac.kr

Abstract. To guarantee secure communication in wireless sensor networks, secret keys should be securely established between sensor nodes. Recently, an efficient security mechanism was proposed for large-scale distributed sensor networks by Zhu, Setia, and Jajodia. In their scheme, each node uses a single initial key to establish pair-wise keys and erases the key after key setup. If the key is compromised during key setup, however, the entire network will be compromised. Therefore, the performance overhead during key setup is very important for the speedy key establishment. In this paper, we propose a modified scheme which reduces the performance overhead during key setup and has provable security after key setup.

Keywords: security, key management, wireless sensor networks

1 Introduction

Wireless sensor networks are well recognized as a new paradigm for future communication. Sensor networks consist of a huge number of battery powered and low-cost devices, called sensor nodes. Each sensor node is equipped with sensing, data processing, and communicating components [1,3].

To provide secure communication within wireless sensor networks, it is essential that secret keys should be securely established between sensor nodes. The shared secret key may later be used to achieve some cryptographic goals such as confidentiality or data integrity. However, due to limited resources of sensor nodes, the traditional schemes such as public key cryptography are impractical in sensor networks. Furthermore, the position of sensor nodes (hence, the neighbors of nodes) cannot be pre-determined since they are randomly deployed in unattended areas. Due to this restriction, most schemes are based on the pre-distribution of potential keys.

Another security concern in sensor networks is resilience against node capture. Sensor nodes are deployed randomly in hostile areas where they are exposed to the risk of physical attacks. For instance, an attacker can capture sensor nodes to obtain secret information stored within memory of the nodes. The ultimate

* This work was supported by the Brain Korea 21 Project in 2006.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 437–446, 2006.

goal may be to acquire *perfect resilience* [4] which means that even if a node is captured, it provides no information about links that it is not directly involved in.

Related Works. When we consider the design of key distribution schemes, the simplest method is to embed a single network-wide key in the memory of all nodes before nodes are deployed. In this case, however, the entire network can be compromised if a single node is captured. Another extreme method is that each node in a network of n nodes shares a unique pair-wise key with every other node in the network before deployment. This requires memory for $n - 1$ keys for each sensor node. Therefore, these two methods are unsuitable for wireless sensor networks.

Perrig et al. presented SPINS [10], security protocols for sensor networks. In SPINS, each node shares a secret key with a base station and establishes its pair-wise keys through the base station. This architecture satisfies the small memory requirement and offers perfect resilience against node capture. However, because the base station should participate in every pair-wise key establishment, SPINS requires significant communication overhead and does not support large-scale networks.

Zhu et al. presented LEAP [11], an efficient key management method. All the nodes in LEAP save an initial key before deployment. After deployment, each node establishes a pair-wise key from the initial key and then erases the initial key securely. Although LEAP is very efficient, it must assume that it is difficult for the initial key to be exposed by node capture during initial key setup.

Eschenauer and Gligor presented a random key pre-distribution scheme for pair-wise key establishment [8] in which a key pool is randomly selected from the key space and a key ring, a randomly selected subset from the key pool, is stored in each node before deployment. A common key in two key rings of a pair of neighbor nodes is used as their pair-wise key. Their scheme has been subsequently improved by Chan et al. [4], Liu and Ning [9], and Du et al. [6,7]. However, these schemes require a significant pre-computation phase as well as a large amount of memory.

Contributions. The main contributions of our approach can be summarized as follows:

- Reduced time and cost to establish pair-wise keys. The security of LEAP depends on the success of attacks during key setup. For this reason, the performance overhead of key setup is very important for security as well as efficiency. Our scheme reduces the possibility of being attacked and consumes less energy by cutting down the time and saving the energy during key establishment.
- Provable security. We prove the security of our scheme after key setup. The proof is based on one outlined by Bellare et al. [2]. Assuming that a message authentication code(MAC) is secure against forgery under a chosen-message attack, our scheme has provable security.
- Scalability. Our scheme is suitable to a large network. We note that other schemes [4,10] with perfect resilience against node capture are not scalable.

To be scalable, SPINS [10] requires significant communication overhead because of the participation of a base station in key setup, and the scheme by Chan et al. [4] requires a large amount of memory for each node.

Organization. The rest of the paper is organized as follows. Section 2 shows the notation used in this paper. We give an overview of LEAP in Section 3. We propose our scheme and analyze its performance and security in Section 4. Finally, we conclude our paper in Section 5.

2 Notation

We list the notations used in the paper below:

Notation	Description
n	the expected number of neighbor nodes within communication radius of a given node
$\|\|$	concatenation operator
K_I	the initial key
K_u	the master key of u
K_{uv}	the pair-wise key between u and v
$E(K, \cdot)$	symmetric encryption function using key K
$F(K, \cdot)$	pseudo-random function using key K
$\mathsf{MAC}(K, \cdot)$	message authentication code using key K

3 LEAP [11]

Unlike previous schemes, LEAP supports four types of keys for each node. The four types of keys are as follows: an individual key, a pair-wise key, a cluster key, and a group key. First, an individual key is a shared key between each node and the base station. Second, a pair-wise key is shared between a node and its neighbor node which is only one-hop away. Third, a cluster key is a key between a node and its all neighbor nodes which are also only one-hop away. Last, a group key is one key shared by all nodes in the network.

We now give a detail of each establishment of four keys. An individual key is pre-loaded into each node before deployment; the security of this key is not considered since we assume the base station to be secure. A group key is also pre-loaded and then updated using cluster keys. A cluster key is established and updated, using pair-wise keys. Therefore, it is the security of pair-wise keys that guarantees the security of LEAP.

Now, we will describe the four phases to establish pair-wise keys for sensor nodes.

Key Pre-distribution. Before nodes are deployed, the same initial key K_I is stored on each node. Each node can derive a master key $K_u = F(K_I, u)$, using the initial key with a pseudo-random function.

Neighbor Discovery. After deployment, each node broadcasts a message consisting of its ID and a nonce it selects randomly. In return, neighbor nodes retransmit their ID and MAC that is constructed using their master key. The source is authenticated by verifying the MAC.

$$\begin{aligned} u \longrightarrow * : &\quad u, Nonce_u \\ v \longrightarrow u : &\quad v, \mathsf{MAC}(K_v, Nonce_u || v) \end{aligned}$$

Pair-wise Key Establishment. After source authentication, the pair-wise key in each node is established through information from the neighbor nodes and a pseudo-random function. Nodes u and v use their pair-wise key as $K_{uv} = F(K_v, u)$.

Key Erasure. After key setup, the initial key K_I and all the master keys of neighbor nodes are completely erased.

When a pair-wise key is established in LEAP, there is an assumption that $T_{min} > T_{est}$. The T_{min} is the minimum time that it takes an attacker to obtain secret information from a sensor node. The T_{est} is the time required for the deployed nodes to actually detect their neighbor nodes. This assumption shows that pair-wise keys are established before an attacker captures some nodes and obtains critical information from them. It is needed to check whether this assumption is practicable or not. The transmission rate is 19.2kbps [5] and the transmitted message is very short (a total of 12 bytes when the node ID and its MAC are 4 bytes and 8 bytes respectively). Hence, the assumption is persuasive in the case where the nodes are initially deployed in the network.

4 Our Scheme

In LEAP, the entire network will suffer a severe loss if an initial key is exposed to an attacker during key setup. Hence, early key establishment must be completed quickly in order to strengthen the security of LEAP.

4.1 Initial Key Setup

In LEAP, each node executes communication at $O(n)$ until the initial key is deleted, whereas in our scheme, the communication required in each node is a single broadcast in the neighbor discovery phase. In general, more time and more energy are required in communicating than computing the symmetric functions. In an example of SPINS [10], the communication cost is about 97% while computation cost is just less than 3%. Therefore, it is much more efficient to reduce the communication cost than to improve the computation cost. Therefore our experiment is very meaningful. The four phases to establish a pair-wise key are as follows:

Key Pre-distribution. In our scheme, like LEAP, a single initial key K_I is pre-loaded in all the nodes before deployment. A sensor node u computes its master key $K_u = \mathsf{MAC}(K_I, u)$ that will be used later to establish pair-wise keys with new nodes.

Neighbor Discovery. The sensor node u selects a nonce $Nonce_u$ randomly and computes a MAC value such as $\mathsf{MAC}(K_I, Nonce_u||u)$. Then, the sensor node broadcasts a message consisting of its node ID, $Nonce_u$, and $\mathsf{MAC}(K_I, Nonce_u||u)$. After this phase, all the nodes in the network can obtain the IDs of their neighbor nodes. As each node verifies the MACs of its neighbor nodes, it can authenticate the initial key and their IDs. In LEAP, the master key of each node is used as a MAC key but it is sufficient to use the initial key as the MAC key because an attacker who cannot derive a master key is also unable to know the initial key.

Pair-wise Key Establishment. Collecting the IDs of its neighbor nodes, node u can compute $K_{uv} = \mathsf{MAC}(K_I, u||v)$ to use as a pair-wise key with its neighbor node v (if $u < v$). The pair-wise key is directly derived from the initial key without computing the master key of its neighbor nodes.

Key Erasure. In this phase, each node erases the initial key.

This scheme improves the security and efficiency of LEAP. In the neighbor discovery phase, our scheme requires a single broadcast so that the amount of communication is reduced considerably. Also, in LEAP, each node has to derive the master key of neighbor nodes to verify their MACs while this is not necessary in our scheme in that we generate the MAC with an initial key. Hence, in our scheme, both communication and computation costs are reduced.

Now that the broadcast message includes MAC values, the neighbor nodes can verify whether the party is sound through each other MAC values. In case that key confirmation is needed between the neighbor nodes, any future messages encrypted and authenticated with the pair-wise key can implicitly achieve the same effect.

4.2 Node Addition After Initial Key Setup

For a very large sensor network, node addition must be feasible anytime. In LEAP, it is difficult for a new node to establish a pair-wise key with old nodes because old nodes erased the initial key after key setup. However it is possible to establish a pair-wise key with old nodes using the master key derived from the initial key and their ID.

$$\begin{aligned} w \longrightarrow u: &\quad w, Nonce_w \\ u \longrightarrow w: &\quad u, \mathsf{MAC}(K_u, Nonce_w||u) \end{aligned}$$

A new node w is deployed with the initial key K_I pre-loaded. The new node w detects its old neighbor node u and can establish the pair-wise key $K_{wu} =$

$F(K_u, w)$ from master key $K_u = F(K_I, u)$ of u. This method does apply to our scheme except the pair-wise key $K_{wu} = \mathsf{MAC}(K_u, w)$ between the new node w and the old node u.

The new node can quickly establish the pair-wise key with working nodes but not with sleeping nodes without some delay. The reason is that sleeping nodes cannot respond to the request of the new node until their state changes from sleeping mode to working one. If working nodes inform a new node of their neighbor nodes, the new node can establish pair-wise keys in advance through collecting IDs of sleeping nodes before sleeping nodes change their mode to working one. In that case, it is needless for new node to save the initial key until sleeping nodes convert to working mode. Therefore, the new node can establish pair-wise keys with its neighbor old nodes. In our scheme, the addition method of LEAP can be used since old nodes have the master key derived from the initial key and their ID.

4.3 Performance Analysis

Zhu et al presented a technical report about LEAP [12]. In this report, they implemented LEAP with the following algorithms on the TinyOS platform. First, the linear-feedback shift register(LFSR) was employed to generate the pseudo-random numbers. The RC5 block cipher was used for encryption along with CBC-MAC.

Also, MAC replaced both the pseudo-random functions and the one-way functions in order to lessen the space of code in the ROM. As a result, RC5 was used for all the operations - the encryption function, CBC-MAC, the pseudo-random function, and the one-way function. Our scheme also employs a MAC function in place of a pseudo-random function for the same reason.

Comparing the computation cost during initial key setup, LEAP needs the $2n$ operations for the MAC function and another $2n$ operations for the F function. Since the F function in LEAP was replaced with the MAC function, the total number of operations for the MAC function would eventually be $4n$, while the total number of operations for the MAC function in our scheme is just $2n + 1$. Conclusively, in our scheme, computation overhead is two times more efficient than in LEAP and the efficiency of communication overhead is also about $0.75n$ times better. The table below compares the two schemes when the node ID and the nonce are each 4 bytes and the MAC is 8 bytes.

Table 1. Comparison of Communication Overhead

	Broadcast Communication	**Unicast Communication**
LEAP	$1 \times (\ 8\ byte\ )$	$n \times (\ 12\ byte\ )$
Our Scheme	$1 \times (\ 16\ byte\ )$	0

4.4 Security Analysis

In both schemes, LEAP and our scheme, the entire network will sustain a serious loss under the situation of exposing the initial key. However, our scheme has

less probability of exposing the initial key because the performance overhead in our scheme, including the computation and communication overhead, is more improved than in LEAP during the key setup.

In our scheme, after key setup, the information in captured sensor nodes cannot be used to find any information about shared keys between non-captured sensor nodes. We assume that an attacker captures nodes in which initial key has been erased after key setup. Hence, she cannot acquire K_I, but can obtain MAC values which were generated using K_I. In this scenario, she attempts to acquire master keys or pair-wise keys of non-captured nodes by computing them either directly or indirectly. First, if she computes K_I from the master key $\mathsf{MAC}(K_I, u')$ or the pair-wise key $\mathsf{MAC}(K_I, u'||v')$ of a captured node u', she could acquire master key $\mathsf{MAC}(K_I, u)$ or pair-wise key $\mathsf{MAC}(K_I, u||v)$ of a non-captured node u, where v' is a neighbor of u' and v is a neighbor of u. However, this is impossible due to the one-way property of MAC functions. Second, if there are some methods for indirectly computing only master key $\mathsf{MAC}(K_I, u)$ or pair-wise key $\mathsf{MAC}(K_I, u||v)$ without using K_I, our scheme will be insecure.

To formally prove the security of our scheme, we first review the security of message authentication codes defined in [2]. A message authentication code takes as inputs a key K and a message M, and outputs a string σ.

$$\mathsf{MAC} : Key(\mathsf{MAC}) \times Dom(\mathsf{MAC}) \longrightarrow \{0,1\}^k$$

The key K is shared between a sender and a receiver. When the sender wants to send a message M it computes $\sigma = \mathsf{MAC}(K, M)$ and transmits the pair (M, σ) to the receiver. The receiver re-computes $\mathsf{MAC}(K, M)$ and verifies that this equals the value σ. An attacker is allowed to mount a *chosen message attack*(cma) in which it can obtain MACs of messages of its choice. If it outputs a valid pair (M, σ) which was not a query to its MAC oracle, then it will be considered successful.

Definition 1. Consider the following experiment.

Experiment $\mathsf{Forge}^{\mathsf{cma}}_{\mathsf{MAC}}(A)$
$K \overset{R}{\leftarrow} Key(\mathsf{MAC})(k)$
$(M, \sigma) \leftarrow A^{\mathsf{MAC}(\mathsf{K},\cdot)}$
If $\mathsf{MAC}(K, M) = \sigma$ and M was not a query of A to its oracle
then return 1 else return 0

Now let $\mathsf{Succ}^{\mathsf{cma}}_{\mathsf{MAC}}(A) \overset{def}{=} Pr[\mathsf{Forge}^{\mathsf{cma}}_{\mathsf{MAC}}(A) = 1]$. Then an advantage function of MAC is defined as follows:

$$\mathsf{Adv}^{\mathsf{cma}}_{\mathsf{MAC}}(q, t) \overset{def}{=} \max_{A}\{\mathsf{Succ}^{\mathsf{cma}}_{\mathsf{MAC}}(A)\}$$

where the maximum is taken over all A with execution time t and at most q queries to the oracle $\mathsf{MAC}(K, \cdot)$. A message authentication code will be secure against *chosen message attack* if the advantage is negligible in the security parameter k.

We define the security of key management schemes against node capture in sensor networks. An attacker is allowed to mount a *chosen node capture attack*(cna) in which it can obtain master keys and pair-wise keys of captured nodes. If it outputs a key of a master key or a pair-wise key of an non-captured node, then it will be considered successful.

Definition 2. We model wireless sensor networks as a directed graph $G = (N, E)$ where $N = \{u_1, u_2, \cdots, u_{|N|}\}$ and $E = \{\langle u, v\rangle : u, v \text{ are neighbors and } u < v\}$. Let n be the expected degree of a node in G.

Definition 3. A sensor key management scheme (M) is secure against *chosen node capture attack* if the following advantage is negligible in the security parameter k. An attacker is allowed to use oracle $\mathsf{M}(\mathsf{G}, \mathsf{K}, \cdot)$ which for an input query $u' \in N$, responds $str \in \{0,1\}^{k(1+n)}$ which contains $(u', \mathsf{MAC}(K, u'))$ and (u', v', σ') where $\sigma' = \mathsf{MAC}(K, u'||v')$ if $\langle u', v'\rangle \in E$ or $\sigma' = \mathsf{MAC}(K, v'||u')$ if $\langle v', u'\rangle \in E$.

Experiment $\mathsf{Compro}^{\mathsf{cna}}_{\mathsf{M}}(B)$
$K \stackrel{R}{\leftarrow} Key(\mathsf{M})(k)$
Generate G as defined in Definition 2.
G is given to B
$(u, \sigma) \vee (u, v, \sigma) \leftarrow B^{\mathsf{M}(\mathsf{G},\mathsf{K},\cdot)}$
If $(((u, \sigma) \wedge \mathsf{MAC}(K, u) = \sigma) \vee ((u, v, \sigma)$
$\wedge((\mathsf{MAC}(K, u||v) = \sigma \wedge u < v) \vee (\mathsf{MAC}(K, v||u) = \sigma \wedge v < u))))$
$\wedge(u, v$ were not a query of B to its oracle)
then return 1 else return 0

Now let $\mathsf{Succ}^{\mathsf{cna}}_{\mathsf{M}}(B) \stackrel{def}{=} Pr[\mathsf{Compro}^{\mathsf{cna}}_{\mathsf{M}}(B) = 1]$. Then an advantage function of M is defined as follows:

$$\mathsf{Adv}^{\mathsf{cna}}_{\mathsf{M}}(q', t') \stackrel{def}{=} \max_{B}\{\mathsf{Succ}^{\mathsf{cna}}_{\mathsf{M}}(B)\}$$

The maximum is taken over all B with execution time t' and at most q' queries to the oracle.

The following theorem means that she cannot compute MAC values of non-captured nodes from MAC values of captured nodes if the message authentication code is secure.

Theorem 1. Let $\mathsf{MAC} : Key(\mathsf{MAC}) \times Dom(\mathsf{MAC}) \longrightarrow \{0,1\}^k$ be a family of functions, and let $q, t, q', t' \geq 1$ be integers. Let M be the proposed scheme. Then

$$\mathsf{Adv}^{\mathsf{cna}}_{\mathsf{M}}(q', t') \leq \mathsf{Adv}^{\mathsf{cma}}_{\mathsf{MAC}}(q, t)$$

where $q \leq q' \cdot (1 + n)$ and $t = t' + O(k)$.

Proof) Let B be an attacker breaking M. We construct an attacker A_B breaking MAC. Consider the following experiment.

Attacker $A_B^{\mathsf{MAC}(K,\cdot)}$

Generate $G = (N, E)$
G is given to B
Run attacker B, replying to its oracle queries as follows:
While B asks a query u' to the oracle do
Generate $str \in \{0,1\}^{k(1+n)}$ for a expected degree n of a node such that
1. $(u', \mathsf{MAC}(K, u'))$ is in str,
2. for each $\langle u', v' \rangle \in E$, $(u', v', \mathsf{MAC}(K, u'||v'))$ is in str, and
3. for each $\langle v', u' \rangle \in E$, $(v', u', \mathsf{MAC}(K, v'||u'))$ is in str.
Return str to B as an answer
EndDo
B stops and outputs (u, σ) or $((u, v, \sigma)$ or $(v, u, \sigma))$
A returns the output of B

Here A_B is running B and provides answers to B's oracle queries. When B asks a node capture query u', attacker A_B needs to return str which is the memory information of node u'. B returns (u, σ) or $((u, v, \sigma)$ or $(v, u, \sigma))$ which is a valid forgery of MAC. So, we have

$$\mathsf{Succ}_{\mathsf{M}}^{\mathsf{cna}}(B) \leq \mathsf{Succ}_{\mathsf{MAC}}^{\mathsf{cma}}(A_B). \tag{1}$$

Inequality of the theorem is obtained as follows:

$$\begin{aligned} \mathsf{Adv}_{\mathsf{M}}^{\mathsf{cna}}(q', t') &= \max_{B}\{\mathsf{Succ}_{\mathsf{M}}^{\mathsf{cna}}(B)\} \\ &\leq \max_{B}\{\mathsf{Succ}_{\mathsf{MAC}}^{\mathsf{cma}}(A_B)\} \\ &\leq \max_{A}\{\mathsf{Succ}_{\mathsf{MAC}}^{\mathsf{cma}}(A)\} \\ &= \mathsf{Adv}_{\mathsf{MAC}}^{\mathsf{cma}}(q, t). \end{aligned}$$

The maximum, in the case of B, is taken over all adversaries whose resources are q', t'. In the second line, we apply Inequality (1). ■

5 Conclusion

We presented a new key scheme for large-scale distributed sensor networks. Our scheme has the following properties. First, compared to LEAP, our scheme is significantly more efficient and secure. Second, we prove the security of our scheme after key setup. Finally, our scheme supports large-scale networks because performance overhead in our scheme is independent of network size. Unlike other scheme [4,6,7,8,9], both our scheme and LEAP have perfect resilience against node capture after key setup. However, since they are weak during key setup, this paper was focused on designing an efficient key establishment scheme.

References

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", In Proceedings of the IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002.
2. M. Bellare, J. Kilian, and P. Rogaway, "The security of the cipher block chaining message authentication code", Journal of Computer and System Sciences, Vol. 61, No. 3, pp. 362-399, December 2000.
3. D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and approaches for distributed sensor network security", NAI Labs Technical Report 00-010, September 2000.
4. H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks", In Proceedings of the 2003 IEEE Symposium on Security and Privacy, pp. 197-213, May 2003.
5. Crossbow technology inc. URL: http://www.xbow.com.
6. W. Du, J. Deng, Y. S. Han, S. Chen, and P.K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge", In Proceedings of the IEEE INFOCOM '04, pp. 586-597, March 2004.
7. W. Du, J. Deng, Y. S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks", In Proceedings of the ACM Transactions on Information and System Security, pp. 228-258, August 2005.
8. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", In Proceedings of the 9th ACM conference on Computer and communications security, pp. 41-47, November 2002.
9. D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks", In Proceedings of the ACM Transactions on Information and System Security, pp. 41-77, February 2005.
10. A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security protocols for sensor networks", In Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking, pp. 189-199, July 2001.
11. S. Zhu, S. Setia, and S. Jajodia. "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", In Proceedings of the Tenth ACM conference on Computer and Communications Security, pp. 62-72, October 2003.
12. S. Zhu, S. Setia, and S. Jajodia. The technical report about LEAP, URL: http://www.cse.psu.edu/ $\sim$ szhu/research.htm, August 2004.

A Quadtree-Based Data Dissemination Protocol for Wireless Sensor Networks with Mobile Sinks*

Zeeshan Hameed Mir and Young-Bae Ko

Graduate School of Information and Communication,
Ajou University, Suwon, Republic of Korea
{zhmir, youngko}@ajou.ac.kr

Abstract. The envisioned sensor network architecture where some of the nodes may be mobile poses several new challenges to this special type of ad hoc wireless network. Recently, researchers have proposed several data dissemination protocols based on some hierarchical structure mainly constructed by a source node to support mobile sinks. However, such a source-initiated hierarchical structure results in significant resource consumption as the number of source-sink pairs are increased. Additionally, stimulus mobility aggravates the situation, where several sources may build a separate data forwarding hierarchy along the stimulus moving path. In this paper, we propose a new data dissemination protocol that exploits "Quadtree-based network space partitioning" to provide more efficient routing among multiple *mobile* stimuli and sink nodes. Simulation results show that our work significantly reduces average energy consumption while maintaining comparably higher data delivery ratio.

Keywords: Wireless Sensor Networks, Mobility, Quadtree-based scheme.

1 Introduction

A wireless sensor network (WSN) consists of a number of tiny sensors that are densely deployed to monitor and interact with the physical world [1] [2]. Since each sensor can partially observe the large terrain, they must collaborate for efficient and reliable delivery of sensory data to the users (i.e., sinks). Sensor network systems spur an immense research potential for a wide range of new applications. One of the applications would be an agriculture production [3], for which the opportunity for sensor networks is explored to aid in a mobile work environment. Here, a mobile worker might be a robot or human equipped with sensor(s) collecting and transmitting data to the sink. Alternatively, static nodes can collectively track any moving target (i.e., stimulus) they detect and forward data through multi-hop communication towards the mobile sink.

* This research was in part supported by Ubiquitous Autonomic Computing and Network Project, IT Foreign Specialist Inviting Program, and ITRC (IT Research Center) Support Program, all supervised by IITA(Institute of Information Technology Assessment), the Ministry of Information and Communication (MIC), Korea.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 447–458, 2006.

Until recently, most of the research on data dissemination in WSN has focused on delivering data to *stationary* sinks. Sink mobility have been considered as a source of adversary to large-scale sensor networking, because the sink nodes are required to propagate their current position continuously so that future reports can be forwarded accordingly. In gradient-based routing protocols such as Directed Diffusion [4] and its variants, reverse paths are established among all the source-sink pairs based on some reverse path vector. This is achieved by periodically flooding control packets by sink nodes, which may cause significant overhead. Moreover, the reverse path vector changes with sink mobility which often causes more frequent flooding. In order to support sink mobility [5] and [6] proposed source-initiated hierarchal structure to the number of stationary or mobile sinks. However, the overhead of per source node grid construction and maintenance make these solutions unsuitable in presence of mobile stimulus.

In our proposed scheme, named as "Quadtree-based Data Dissemination (QDD)", a common hierarchy of data forwarding nodes is created by Quadtree-based partitioning of physical space into successive quadrants. Earlier, this approach has been utilized for addressing the sensor network field using location-based bit strings that represent the Quadtree address of the node [7]. In our approach, upon detecting a mobile stimulus, a source node calculates a set of rendezvous points by successively partitioning the sensor network space into four equally sized logical quadrants, and sends data packets to the nodes closer to the centroid of each successive partition. The mobile sink follows the same strategy for the data query packet dissemination. It starts from querying the immediate rendezvous node and continues until it finds the required data report. Since this procedure results in selecting same static sensor nodes, they form a common hierarchy for information forwarding and therefore results in lower overhead. The simulation results confirm that the cost of using separate hierarchy is considerably higher than our approach in terms of energy consumption, while the data delivery ratio is comparable for both approaches.

The remainder of the paper is organized as follows. Related work on data dissemination in WSN is covered in Section 2. Section 3 introduces our scheme, followed by simulation study in Section 4. In Section 5 we comment on certain design issues and future work. Finally, conclusion is provided in Section 6.

2 Related Work

Efficient and reliable collaboration among sensor nodes is a key to success for all types of applications in large-scale wireless sensor networks. The decision about how these sensor nodes communicate has a significant impact on the energy and bandwidth consumption [1] [2]. Furthermore, a particular architecture of mobile sensor networks will pose several new challenges.

Directed Diffusion [4] has been proposed as a distributed event detection mechanism for sensor networks. Motivated by the fact that the majority of data transmissions are destined in the direction of a sink, each sensor node sets up a *gradient* i.e., a direction state, towards its neighboring nodes in response to

sink's periodic flooding of interest packets. The sink node can be reached by traversing a high quality reverse path, selected among possibly multiple paths as the result of path reinforcement mechanism. Gradient-based Routing (GBR) [8] and Gradient Broadcast (GRAB) [9] took advantage of the freedom Directed Diffusion paradigm offers by attaching different semantics to the value of gradient. A common assumption each of these gradient-based data dissemination protocols make is the diffusion of gradient value throughout the sensor network, which costs significantly high in terms of overall routing overhead. Sink mobility adds further challenges, where it is essential for reliable data dissemination to maintain correct value of the gradient by a sink.

In TTDD [5], each source node constructs a uniform grid structure throughout the sensor field. A sink collects the reports on stimulus by first flooding its query within the local grid cell. The query packet is then traversed along the grid until either it reaches a source or any node that has yet received data from the source. While the query is disseminated over the grid, a reverse path is established towards the sink. In presence of mobile stimulus several sources may build a separate grid along the stimulus path. This situation can lead to excessive energy drain and increased packet collisions. Similar in spirit of the TTDD, Hierarchical Data Dissemination Scheme (HDDS) [6] is based on constructing a different hierarchy of data dissemination nodes from each source to potentially multiple sinks. In their work, a data forwarding node performs a load balancing by making another level of forwarding nodes. However, a scenario with mobile stimulus faces the limitations similar to the TTDD model.

The problem of sensor network space partitioning has been exploited for efficient execution of spatial queries in sensor networks. In [10], a distributed indexing structure based on R-tree spatial data structure is presented that enables querying of information related to a region of interest . However, in our proposed scheme we have utilized Quadtree-based partitioning to provide an efficient solution to the mobile stimulus and sink problem.

3 Quadtree-Based Data Dissemination (QDD)

The main goal of our scheme is to implement an efficient data dissemination protocol that supports both stimulus and sink mobility, by exploiting Quadtree-based sensor network space partitioning. Following are the assumptions our protocol design is based on:

- Sensor nodes are stationary and location aware, however some or all of the stimuli and sink nodes may be mobile. Since, sensor nodes will remain static a GPS-free localization [11] method can be utilized during the network initialization phase, where a node can also learn its one-hop neighbor location.
- Each sensor node knows the total sensor network space area N, given as $2^k \times 2^k$; where $k = \log_2(N)$.
- Greedy geographical forwarding is used for both data and query packet dissemination.

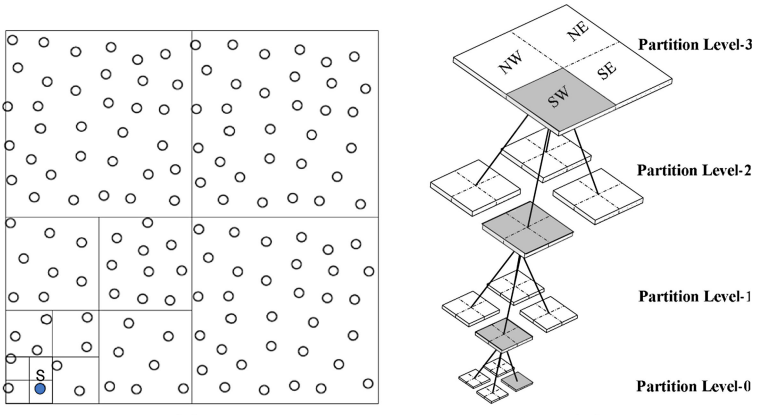


Fig. 1. (a) Sensor network space N partitioning. (b) Quadtree representation.

3.1 Quadtree-Based Network Space Partitioning

In this subsection we describe how the network space partitioning based on the concept of Quadtree is done in our QDD protocol. A sensor node S with location (X_s, Y_s), takes the complete sensor network space N as the root of a Quadtree, and logically partitions N into four equal sized quadrants. Each of these four quadrants North West (NW), South West (SW), North East (NE) and South East (SE) corresponds to a child of N, respectively, such that:

- The root N represents the entire network space, specified by $N.X_{LB} = 1$, $N.Y_{LB} = 1$, $N.X_{UB} = 2^k$ and $N.Y_{UB} = 2^k$; where ($N.X_{LB}$, $N.Y_{LB}$) are coordinates for lower left corner (lower bound) and ($N.X_{UB}$, $N.Y_{UB}$) are coordinates for upper right corner (upper bound) of a square, respectively.
- If P is the parent of child quadrant C, then values for $C.X_{LB}$, $C.Y_{LB}$, $C.X_{UB}$ and $C.Y_{UB}$, depends upon whether C is the NW, SW, NE, or SE child of P.

Next, each quadrant is considered as a separate parent and divided into further four sub-quadrants. Given the current location of node S (X_s, Y_s), this process is repeated for each quadrant, until node S remains the only node in a sub-quadrant (the leaf cell). This method requires a comparison at each partition level, to check if the current sub-quadrant is the leaf cell [7]. For example, if node S is in the NW quadrant of parent P (i.e., C = P.NW), then:

$$\{S \in P.NW{:}(C.X_{LB} \leq X_s \leq C.X_{UB}) \text{ and } (C.Y_{LB} \leq Y_s \leq C.Y_{UB})\}$$

Fig. 1(a) and (b) illustrate the network space partitioning into sub-quadrants by some node S and the corresponding Quadtree representation.

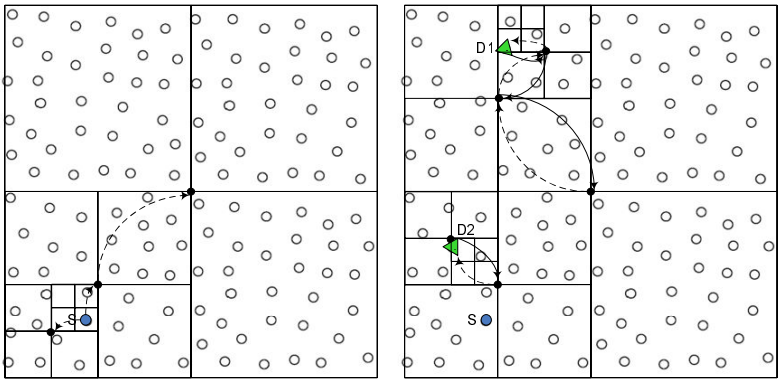


Fig. 2. (a) Rendezvous points and data packet forwarding by source node S (dashed lines). (b) Query packet forwarding by sink nodes D1 and D2 (solid lines).

3.2 Data Forwarding

The simplicity of our scheme is in the way a source node disseminates data. Upon detecting a stimulus, source node S performs a logical partitioning of sensor network field as explained in the previous section. For each partition level i represented by a square with lower corner and upper corner values set to (i.X_{LB}, i.Y_{LB}) and (i.X_{UB}, i.Y_{UB}) respectively, it calculates a list of central points called *rendezvous points* RP (x_i, y_i), given as:

$$x_i = \text{i.}X_{LB}+(\text{i.}X_{UB} - \text{i.}X_{LB})/2$$
$$y_i = \text{i.}Y_{LB}+(\text{i.}Y_{UB} - \text{i.}Y_{LB})/2 \ (0 < \text{i} \leq \text{k})$$

Fig. 2(a) shows the rendezvous points calculated by node S and the data forwarding process. It starts from its current location as the first rendezvous point (0^{th} level) and forwards data packet to the *immediate rendezvous point* (1^{st} partition level) using geographical greedy forwarding. If S is not itself the closest node to the immediate rendezvous point it looks into its neighbor table for a neighbor that is closest to that point and forward packet to it. Each node in turn repeats this process, until a node finds that no other node in its neighborhood is closer than itself. Now this node becomes the *rendezvous node*.

While forwarding data packets, each rendezvous node maintains a local table, including the source node's current location and identity, data message M, the previous rendezvous node's location, packet type and the sequence number, so that the duplicate entries related to same data packet can be identified and subsequently dropped. In addition, each table entry includes an expire field, that determines how long that entry would remain valid before it is discarded from the table.

3.3 Query Forwarding

Consider an application that tracks location and type of activity in a mobile work environment. When a stationary or mobile sink requires sensory data it calculates a list of rendezvous points and sends a query packet towards its immediate rendezvous point. On receiving a query packet, the immediate rendezvous node checks its local table for a valid data (that meets the criteria specified within the query packet and that is not expired yet). If this lookup for requested data fails, the query is propagated one level up in the hierarchy until it reaches either an intermediate rendezvous node that has the requested data or the k^{th} partition level rendezvous node.

Fig. 2(b) exemplifies the query forwarding process, where two sink nodes D1 and D2 query for the data generated by source node S. This figure shows two different scenarios for query forwarding. Each sink sends query packets towards their respective immediate rendezvous point. As each rendezvous node receives the query packet, it checks for any valid data sink nodes are looking for. Based on its findings, it either sends the data packet towards the rendezvous point that is known to be closest to the sink (sink D2 in this case) or forwards the query packet one level up in the hierarchy, where it can find the requested data at the k^{th} level of the hierarchy (sink D1, for example). As soon as a query matches with the required data in the local table, data is forwarded towards the sink by traversing the reverse path established during the query dissemination process.

Due to a random deployment of sensor nodes, there might exist two different nodes: one for holding data packets and the other for query packets. This situation can occur due to the following two reasons. For the first case, when there are several nodes close to the rendezvous point and therefore more than one node become candidates for keeping information, we have set a minimum distance threshold value to tell if it is the same location. Secondly, a network partitioning also results in this situation. Depending on the network neighborhood density, we set a maximum distance threshold for a node to become a rendezvous node. While forwarding packets towards the rendezvous point RP, if a node finds none of its neighbors closer than itself and its distance from RP is greater than this value it simply performs one-hop flooding.

Generally, there are two possible choices for a sink to receive data packets, either a single event or multiple continuous events. In the former case each query by a sink is acknowledged with the requested data only once whereas in the later case a sink receives multiple data continuously in response to its query. In order to receive continuous data packets, rendezvous nodes also maintain the query entries in their local table. The purpose behind storing these entries is twofold. First, while the query packet traverses the hierarchy of rendezvous points, it establishes a backward path towards the sink and secondly to reduce the amount of time, sink node has to wait for newly announced data. Upon receiving a new data packet from the source, a rendezvous node immediately forwards it towards the sink by following the path stored in local table. The degree of how long these entries remain persistent is controlled by the frequency with which sink nodes

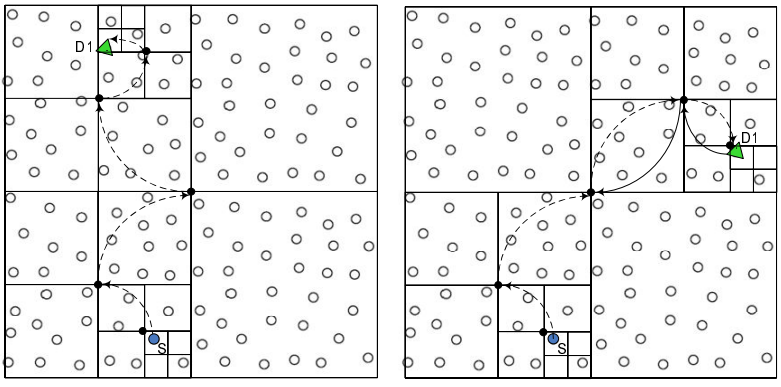


Fig. 3. (a) Stimulus mobility scenario (b) Sink D1 mobility scenario

transmit query packets. Each query packet refreshes the query entries in table with the location of the last rendezvous point that is serving the sink and the amount of time those entries will remain valid (for example, a query might have a DURATION clause that specifies query lifetime).

Here it is noteworthy that how this scheme accommodates stimulus and sink mobility without any associated overhead and delays. Each time a mobile sink has to inquire about any new updates; it just needs to send its query packet up to that level where the latest updates are available. On the other hand, a source node sends data to the set of calculated rendezvous points. Since the sensor nodes are immobile the information flows through same intermediate rendezvous nodes. Fig. 3(a) and Fig. 3(b) show two different network setups as a result of stimulus and sink mobility.

4 Performance Evaluation

For the purpose of performance evaluation, we have performed extensive simulations. A comparative study is carried out with TTDD model by varying the number of source-sink pairs. Then, the impact of stimulus mobility on the proposed scheme is shown as a function of maximum stimulus speed. The set of experiments presented here describe results obtained by evaluating our scheme in the presence of multiple mobile stimuli and sink nodes.

4.1 Simulation Environments

We have implemented and tested our protocol performance in ns-2 [12]. In order to ensure a fair comparison with the TTDD model, we set simulation parameters comparable to those used in [5]. This includes simulation of IEEE MAC 802.11 DCF and node energy model which consumes 0.395W, 0.660W and 0.035W per

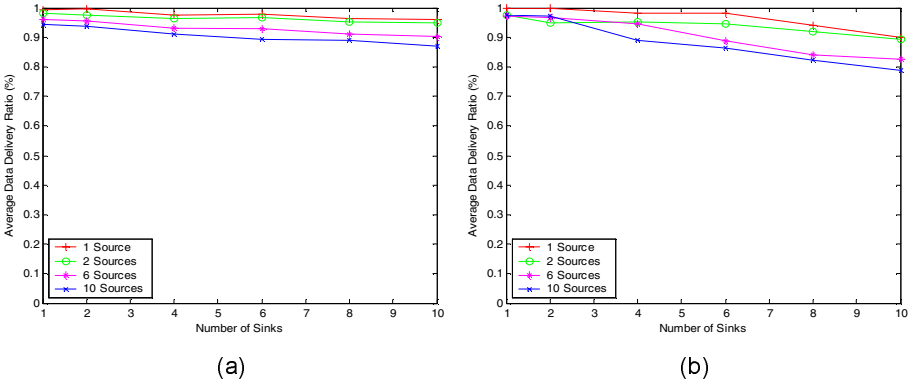


Fig. 4. Comparison in terms of Data Delivery Ratio: (a)QDD and (b)TTDD

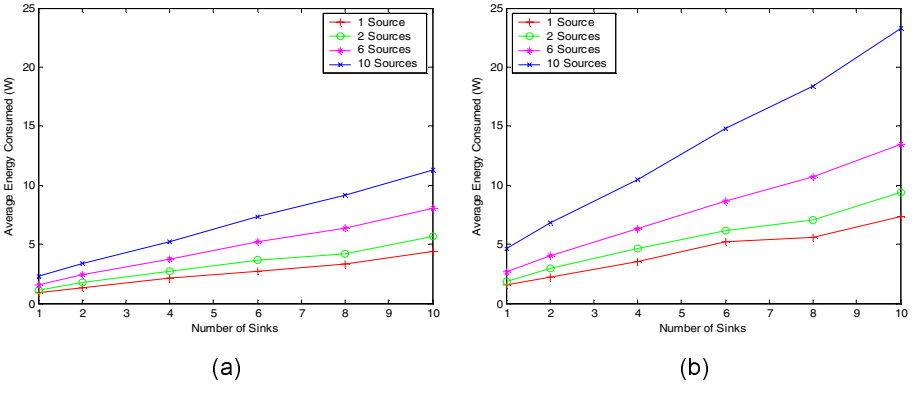


Fig. 5. Comparison in terms of Energy consumed: (a)QDD and (b)TTDD

receiving, transmitting and idle modes, respectively. In our simulation model, 200 sensor nodes are randomly placed on a 2048 x 2048m^2 grid. For different set of simulations, speed and pause time of stimuli and sink nodes vary accordingly with Random Waypoint model used as the mobility model. Total simulation duration is 200 seconds. During simulations the data rate is 1 packet per second, so there are total 200 data packets sent. All the simulation results are averaged over six different scenarios. Following metrics are used to evaluate our proposed scheme. (a) *Average Data Delivery Ratio*, obtained by comparing total number of data reports received by a sink with total packets generated by a source, which is further averaged over total number of source-sink pairs. (b) *Average Energy Consumed*, represented as the ratio between the total energy consumed during a simulation run and the total number of sensor nodes. (c) *Average Delay*, defined as the total time elapsed between the data generation by a source node and reception by a sink over total number of data packets received per source-sink pairs.

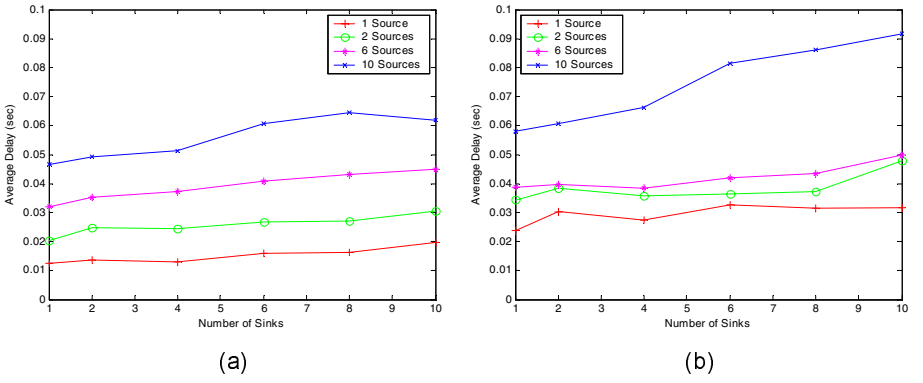


Fig. 6. Comparison in terms of Delay: (a)QDD and (b)TTDD

4.2 Simulation Results

Experiments with Stationary Stimuli and Mobile Sinks: For the first set of simulation results, number of source-sink pairs are varied to make a performance comparison with TTDD scheme in presence of mobile sinks. Mobile sink nodes could attain a maximum speed up to 10m/s with 5 seconds pause time. The stimuli remain static throughout the simulation time. Beginning from the average data delivery ratio Fig. 4(a) and Fig. 4(b), show that for both protocols most of the data packets are delivered. Even though the results are quite comparable, the delivery ratio for TTDD scheme falls more consistently as the number of source-sink pairs grows.

Fig. 5(a) and Fig. 5(b) compare the energy consumption overhead. Here, it demonstrates that the energy requirements of TTDD is substantially higher than that of our scheme. However, for the proposed scheme it increases linearly with the increase in number of sources. In TTDD every source sends data packets to four different corners of each grid cell recursively to build a network wide virtual grid. This practice is in contrast to the way data is disseminated in our scheme, where data packets are required to send to only one rendezvous node per partition level. As the number of source nodes increases, a separate grid structure construction and maintenance on per source basis results in higher cost, both in terms of packet overhead and energy consumption.

Fig. 6 presents the average delay. We can see that in both protocols, the delay increases with the increase in number of source-sink pairs. Once again the reason behind TTDD's delay is the excessive number of data packets sent by source nodes throughout the sensor network and local query packets flooded by the sink nodes. In our case, since all the source and sink nodes forward data along the common hierarchy, incurred delay increase as the number of sources increases. However, the proposed scheme performs better because there is no extra delay associated with tracking mobile sinks.

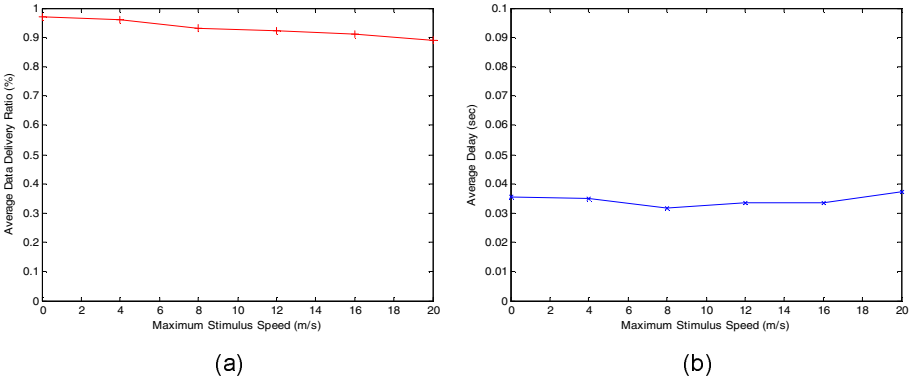


Fig. 7. Impact of stimuli mobility on QDD: (a)Data Delivery Ratio (b)Delay

Experiments with Mobile Stimuli and Sinks: TTDD model has its main focus on scenarios with sink mobility only. In this subsection we describe the impact of stimuli mobility on our protocol as the function of maximum stimulus speed. In these simulation scenarios, stimuli speed varies from 0 to 20m/s where as the sink node speed is chosen randomly between 0 and 10m/s with 5 second pause time for both. For a total of 5 stimuli and 5 sinks deployed, Fig. 7(a) shows the average data delivery ratio. As the stimulus speed increases the delivery ratio decreases gradually. At higher speed stimuli tend to change there immediate quadrants more frequently, however since the higher order partition levels remains the same, therefore most of the data packets are delivered to sink nodes. The average energy consumption statistics remains stagnate at 5W over the changing stimuli speed because of two observations. First of all, the inherent support for stimuli mobility Quadtree-based partitioning offers by making the data delivery to sink nodes independent of the current position of the stimuli and secondly there is no overhead associated with tracking mobile sink. In Fig. 7(b), the average delay increases slightly with speed mainly because the situations where stimuli change quadrants relatively fast. This situation often results in frequent change of lower level rendezvous points and therefore sink queries have to traverse up towards higher levels in hierarchy to fetch data.

5 Discussions

5.1 Distribution of Total Energy Consumed Among Sensor Nodes

Selecting rendezvous nodes based on the geometric argument results in using the same nodes, if needed, to forward information between different source-sink pairs. In order to reduce the risk of exhausting the batteries of these nodes, the responsibility of forwarding data and query packets can be rotated among nodes that are within their close vicinity. Specifically, a rendezvous node can delegate any of its neighboring nodes to handle future traffic for certain period of time and

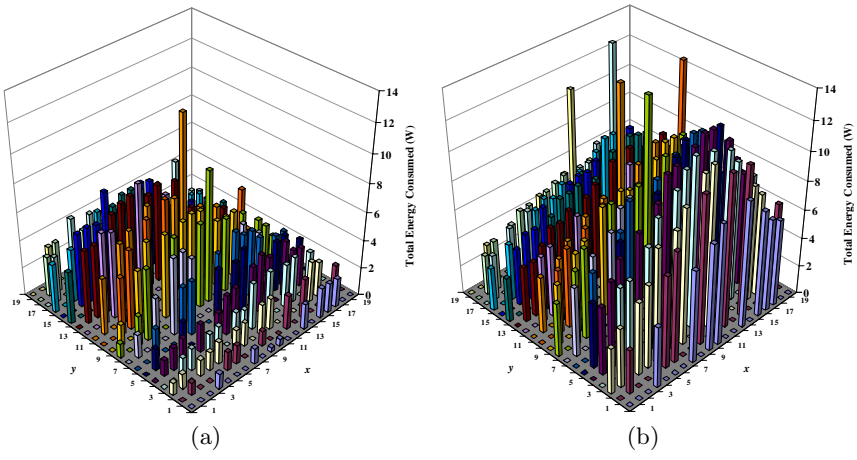


Fig. 8. Distribution of total energy consumed among sensor nodes: (a)QDD (b)TTDD

locally floods its decision to one-hop neighbors. In this way, a packet forwarding node can then use the new designated node for storing data and control entries.

We further studied the distribution of total energy consumed among sensor nodes in the network and contrasted our results with the TTDD model. The simulations are performed with one mobile sink and ten static stimuli, where the itinerary of the sink is randomly selected during the experiments. Sensor network space is divided into 100 x 100m^2 sized non-overlapping blocks for the network size given in the previous section. In Fig. 8(a) and Fig. 8(b), each 3-D bar represents cumulative energy consumed by all the nodes within a block for the proposed scheme and the TTDD model, respectively. Although, energy consumption is highly variable and depends on the current location of the sink, an important observation about our approach is that the nodes that form a common backbone hierarchy experience the highest energy consumption while the energy levels of most of the other nodes remains partially intact. It is therefore, obvious that in our case the network lifetime is defined by a fewer nodes that are along the diagonals of the sensor field. In TTDD, however a separate hierarchy for every source-sink pair is maintained, therefore the energy consumption is equally high throughout the network. This increases the probability to exhaust the battery energy of majority of the nodes, leading to network partitioning and reduced network lifetime.

Moreover, recent studies show that deployment of higher energy and communication capacity nodes can be exploited to leverage the overall system capabilities [13]. The fact that in our scheme the routing decisions are biased to use the common hierarchy can be combined with placement of superior nodes alongside diagonals to further improve the network performance. We leave these design alternatives to be addressed as future work.

5.2 In-network Data Aggregation

Since the forwarding paths along the diagonals of sensor fields are shared among all source-sink pairs, it provides an opportunity for similar data to meet at some common rendezvous point. Data from multiple sources can be aggregated and replaced by a single data packet and forwarded towards the destined sink. Although our proposed scheme can achieve further performance gain by in-network data aggregation, we are intending to explore this avenue in our future work.

6 Conclusion

Environment monitoring application varies greatly with one common goal of detecting and reporting on the phenomena of interest to the sink. In this paper we have proposed an efficient and simple, Quadtree-based data dissemination protocol for large scale wireless sensor networks that supports both stimulus and sink mobility. By making the data dissemination process independent of each others current location, our work provides an efficient solution for mobile stimulus-sink problem. Through simulation results it is shown that a common hierarchy results in reduced communication overhead and significant energy saving against network wide data and control packet transmission overhead.

References

1. D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the World with Wireless Sensor Networks", *Proc. ICASSP'01*, May 2001.
2. D. Estrin and R. Govindan, "Next Century Challenges: Scalable Coordination in Sensor Networks", *Proc. MobiCom'99*, Aug. 1999.
3. J. Burrell, T. Brooke and R. Beckwith, "Vineyard Computing: Sensor Networks in Agricultural Production", *IEEE Pervasive Computing*, 3(1):38-45, Jan. 2004.
4. C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", *Proc. Mobicom'00*, Aug. 2000.
5. F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A Two-Tier Data Dissemination Model for Large-scale Wireless Sensor Networks", *Proc. Mobicom'02*, Sept. 2002.
6. A. Visvanathan, J.H. Youn, and J. Deogun, "Hierarchical Data Dissemination Scheme for Large Scale Sensor Networks", *Proc. ICC'05*, May 2005.
7. C. Cimen, E. Cayirci, and V. Coskun, "Querying Sensor Fields by using Quadtree based Dynamic Cluster and Task Sets", *Proc. IEEE MILCOM'03*, Oct. 2003.
8. C. Schurgers and M. B. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks", *Proc. IEEE MILCOM'01*, Oct. 2001.
9. S. Lu, F. Ye, G. Zhong, and L. Zhang, "Gradient Broadcast: A Robust Data Delivery Protocol for Large-scale Sensor Networks", *Proc. IPSN'03*, April 2003.
10. M. Demirbas and H. Ferhatosmanoglu, "Peer-to-Peer Spatial Queries in Sensor Networks", *Proc. IEEE P2P'03*, Sept. 2003.
11. N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less Low-Cost Outdoor Localization for Very Small Devices", *IEEE Personal Communication*, 7(5):28-34, Oct. 2000.
12. ns-2 network simulator. http://www.isi.edu/nsnam/ns.
13. M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting Heterogeneity in Sensor Networks", *Proc. IEEE INFOCOM'05*, March 2005.

A Virtual Spanner for Efficient Face Routing in Multihop Wireless Networks*

Héctor Tejeda[1], Edgar Chávez[1], Juan A. Sanchez, and Pedro M. Ruiz[2]

[1] Escuela de Ciencias Físico-Matemáticas, Universidad Michoacana, México. {elchavez, htejeda}@fismat.umich.mx
[2] Facultad de Informática, University of Murcia, Spain {jlaguna, pedrom}@dif.um.es.

Abstract. Geographic routing for ad hoc and sensor networks has gained a lot of momentum during the last few years. In this scheme routes are created locally by each individual node, just based on the position of the destination and its local neighbors. To do that, a node selects its best neighbor (according to some metric) out of those being closer than itself to the destination. This operation is called *greedy mode*. When a node has no such neighbors, it enters into *face routing* mode. However, for face routing to work properly, the underlying graph needs to be planarized by removing crossing edges, which may eventually be very good from the routing metric point-of-view. In this paper, we introduce a new localized scheme to build a planar *virtual spanner* in a simple and efficient way, with low control overhead. The produced *virtual spanner* allows *face routing* to be executed, without the need to remove any of the original links in the network. Thus, the best links according to the routing metric can still be used, Our simulation results show that by performing face routing over the virtual spanner, we manage to enhance the routing performance both for greedy-face-greedy routing and face routing between a 40 to 60% compared to existing planarity tests.

1 Introduction

Mobile ad hoc networks (often referred to as MANETs) as well as wireless sensor networks consist of wireless nodes that communicate with each other in the absence of a fixed infrastructure. When a node needs to send a message to another host which is outside of its radio range, it uses other intermediate hosts as relay nodes. Those intermediate nodes are dynamically selected by the routing protocol being used. This kind of networks are useful in many scenarios such as disaster relief, battlefield environments, etc.

Among all routing protocols for these networks, geographic routing [BMSU01] has emerged recently as a very efficient way to provide guaranteed delivery routes without flooding the whole network with control messages. However, nodes are required to be able to know their position and, by exchanging control messages,

* Partially supported by CONACyT and the Spanish MEC by means of the "Ramon y Cajal" program and the SAVIA project (CIT-410000-2005-1).

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 459–470, 2006.

the position of its neighbors. To send a message from the source to the destination, each intermediate node selects locally its *best* neighbor to forward the message towards that destination among those which are closer than itself. Those nodes are often said to provide advance towards the destination. The best node depends on the routing metric. For instance, if we are using hop count as the routing metric, it could be the one which is closest to the destination. This operation is called *greedy mode*. When greedy mode reaches a local minimum (i.e. no neighbor can provide advance towards the destination) then the protocol needs to resort to a recovery mechanism until a node is found which can continue greedy forwarding. This mechanism is *face routing* described in [BMSU01]. The basic idea is that when no progress can be made in greedy mode, packets are sent following the edges of the faces of a planar decomposition of the underlying graph, until greedy mode can again continue, or the destination is eventually reached. This approach combining greedy and face modes when necessary, is commonly known as GFG (Greedy-Face-Greedy) routing [BMSU01]. As we said, the *face routing* part requires the underlying graph to be planar.

There are several methods to extract a planar subgraph from a given Unit Disk Graph (UDG), which models the entire network. A UDG is a graph in which an edge $[u, v]$ exists only if $dist(u, v) \leq r$ being r the radio range. The *Relative Neighborhood graph*, RNG [Tou80] is obtained by applying the RNG test to every edge of the UDG: an edge $[u, v]$ is retained in $RNG(G)$ if there is no vertex z such that $\max\{d_G(u, z), d_G(v, z)\} < d_G(u, v)$. That is, if there is no vertex in the intersection of their disks. The *Gabriel graph*, GG [GS69], applies a slightly different test to every edge of the graph. It retains an edge $[u, v]$ in $GG(G)$ if there is no node in the disk with diameter $\overline{uv}$. Finally, the *Morelia test* [BCG$^+$04] manages to preserve some long edges by using a stronger condition for the removal of edges. An edge $[u, v]$ is not included in $MG(G)$ if there is a couple of points $[x, y]$ so that one of them (or both) is in the disk with diameter $\overline{uv}$ and $[x, y]$ crosses $[u, v]$. Given a UDG G we have $RNG(G) \subseteq GG(G) \subseteq MG(G)$.

The guaranteed delivery provided by *face routing* has a price, which is that the computed routes are generally not optimal. The main reason is that traversing faces to avoid voids, may eventually produce a large deviation from shortest path. Another important reason is that the elimination of links to avoid crossings may degrade the routing performance when the protocol enters into face routing mode. As a matter of fact, long links (which are the ones preferred to reduce hop count) are the ones which are usually eliminated first, because they usually cross many other links.

To mitigate this problem, we propose the creation of a planar virtual spanner of the original graph using a tessellation. Given that crossing edges are forbidden in *face routing* to guarantee correctness of the algorithm, we build our virtual spanner in such a way that guarantees its planarity (there are no crossing virtual edges). Then, when a node enters into *face mode*, it will route using virtual edges, which will then be translated to a path using real nodes. Once the next hop virtual neighbor is selected using face routing, the real nodes will route

the message towards the representative of the selected neighboring tessel. Given that real nodes will route using all available links (no links are eliminated), the performance in face mode of the protocol is enhanced. We shall show this in our simulation results.

The remainder of the paper is organized as follows: Section 2 presents our network model and the problem formulation. Section 3 illustrates how the virtual spanner is built. We explain how to route based on the virtual spanner in section 4. Finally we present some simulation results in section 5 and give some conclusions and future work in section 6.

2 Network Model and Problem Formulation

This section introduces the notation and the model we use throughout the paper. We consider routing algorithms on Euclidean graphs, i.e. weighted graphs where edge weights represent Euclidean distances between the adjacent nodes in a particular embedding in the plane. As usual, a graph G is defined as a pair $G := (V, E)$ where V denotes the set of vertices and $E \subseteq V^2$ denotes the set of edges. The number of nodes is denoted by $n := |V|$ and the Euclidean length of an edge $e \in E$ is denoted by $c_{\mathrm{d}}(e)$. A path $p := v_1, \ldots, v_k$ with each $v_i \in V$ is a list of nodes such that two consecutive nodes are adjacent in G, i.e. $(v_i, v_{i+1} \in E)$. A path p also can be denoted by the corresponding list of edges. In our evaluations we will use the traditional hop count metric. Thus, given a path $p = v_1, \ldots v_k$ the cost of such path is the number of edges traversed.

In this paper we consider the standard UDG model for ad-hoc networks where all nodes have the same transmission range (r). Thus, given two nodes $v_1, v_2 \in V$, the edge $[v_1, v_2] \in E \Leftrightarrow c_{mathrmd}([v_1, v_2]) \leq r$.

As in previous geographic routing works in the literature, we assume that nodes know their positions and those of their neighbors. It is also assumed that sources of data packets know the position of the destination.

3 The Virtual Spanner

We divide the plane in regions with a regular tessellation, which is a tessellation (or planar subdivision) made up of congruent regular polygons. The idea is that an entire region may be represented by a single virtual point, the center of the regular polygon. If we link the centers of the polygons we observe a peculiar behavior: the centers define a dual tessellation that is also planar. The dual of a triangle tessellation is a hexagonal tessellation, while a square tessellation is auto dual.

Only three regular polygons tessellate the Euclidean plane: triangles, squares or hexagons, from elementary geometry. They are depicted in figure 2.

The virtual node for a polygon is chosen as the centroid of the polygon. Two virtual nodes will share an edge if in their respective cells two real nodes are neighbors. Thus, we need to choose a suitable polygon size for building the virtual graph, so that we achieve a good trade-off between the simplicity to build

the virtual graph (guaranteeing that is planar), and the number of cells to be checked in its creation process. We have analyzed three options as we show in figure 1.

a) The transmission radius does not cover all the cell.
b) Any two points in the cell are within radio range.
c) A node in one cell can reach any other node in a neighboring cell.

Case a) complicates the design because it may require multihop routing within a cell. In case c) there may be a very big number of cells in which to look for possible virtual edges. We decided to use case b) because it is the configuration which avoids multihop within a cell in which the number of cells to look for virtual neighbors is low.

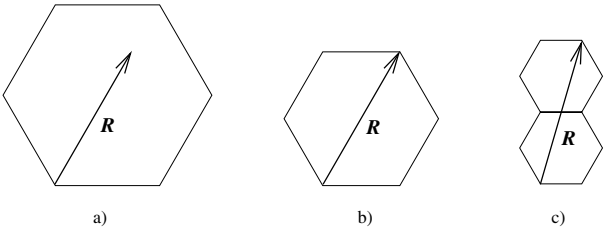
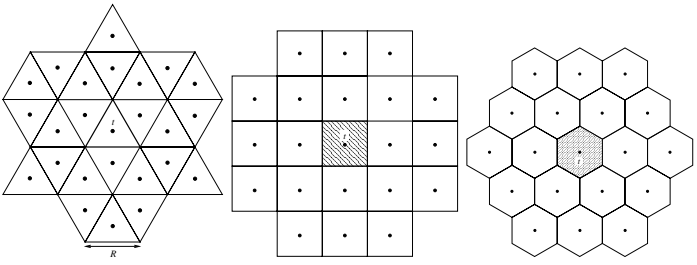


Fig. 1. Variation of polygon size with transmission radius fixed

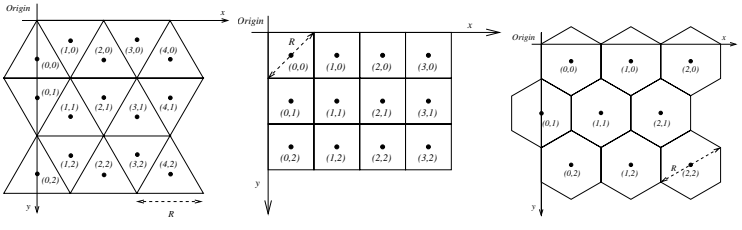
If the graph is dense enough, there will be at least one node in each cell. Thus, each virtual node will be connected to all neighboring virtual nodes. The resulting virtual graph is exactly the dual of the graph, which is planar. In real situations we cannot guarantee that every cell will have a node. Thus, to preserve connectivity we must find all possible virtual neighbors. They may be in cells which are not contiguous to the current one. In figure 2 we show for each different tessellation (triangular, square and hexagonal) the possible cells that may contain nodes which are neighbors of nodes in the current cell t. The cell t can reach more cells when using a triangular configuration (24 cells). With a square configuration 20 cells are candidates and when using hexagonal cells only 18 cells. Please note that the dual of the virtual graph *may not be planar* if we have void cells and want to preserve connectivity. This crossings can be eliminated using a local test, and the complexity of the test depends on the number of neighboring cells.

The grid with triangles, squares or hexagons is located arbitrarily in the plane. Each cell is identified by a coordinate pair as is showed in Figure 3. Note that real nodes only need to know the type of tessellation and the communication radius at deployment time. Based on that, and given their current position they can easily compute the coordinates of their centroid. In addition, only with local information about the position of its neighbors they can compute their local view



(a) Triangles (b) Squares (c) Hexagons

Fig. 2. Regular tessellations in the plane and cell centroids. Additionally, the cells shown are those reachable from t using a radius R equal to the diameter of the cell.



(a) Triangles (b) Squares (c) Hexagons

Fig. 3. Fixing the origin, the virtual coordinates are computed with elementary calculations

of the virtual graph (virtual edges). This has no additional overhead because position of real neighbors is already known or was computed using beacons.

We show below some elementary calculations for the node to compute the coordinates of the virtual node for each real node. It only uses the transmission radius R and its position (x, y).

In addition, each real node also needs to compute the virtual edges shared with reachable cells. Every real node can make exactly the same calculations independtly without the need of a central authority or coordination among them. This connectivity test is accomplished in two stages:

1. Test surrounding cells that are neighbors by their side.
2. Test all other cells that are reachable from current cell but are not neighbors by their side.

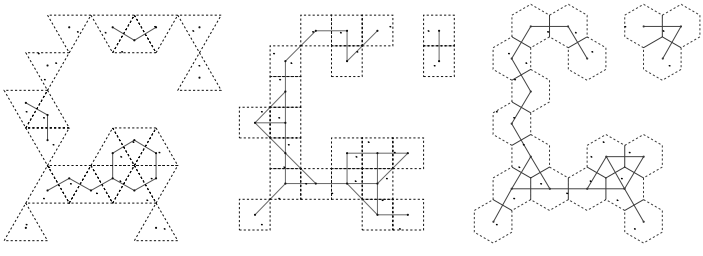
The first stage is easier than the second one because it always produces a planar graph. There are no edge crossings, as it is depicted in figure 4. In the first stage, a virtual edge is added between centroids of two cells adjacent by the side if there are two mutually reachable real nodes, one in each of those

Table 1. Formulas for a node to compute position of its centroid and its tessel

Type of tilling	Position of centroid	Tessel
Hexagonal	$y_c \leftarrow 3R(y+1/3)/4$ **if** $y \bmod 2 = 0$ **then** $x_c \leftarrow \sqrt{3}R(x+1/2)/2$ **else** $x_c \leftarrow \sqrt{3}Rx/2$	$y \leftarrow$**truncate** $(3y_n/4/R)$ **if** $y \bmod 2 = 0$ **then** $x \leftarrow$**truncate** $(2x_n/\sqrt{3}/R)$ **else** $x \leftarrow$**truncate** $((2x_n + \sqrt{3}R/2)/\sqrt{3}/R)$
Triangular	$x_c \leftarrow Rx/2$ **if** $(x+y) \bmod 2 = 0$ **then** $y_c \leftarrow \sqrt{3}R(y+2/3)/2$ **else** $y_c \leftarrow \sqrt{3}R(y+1/3)/2$	$x \leftarrow$**truncate** $(x_n/2/R)$ $y \leftarrow$**truncate** $(2y_n/\sqrt{3}/R)$
Square	$x_c \leftarrow (x+1/2)R/\sqrt{2}$ $y_c \leftarrow (y+1/2)R/\sqrt{2}$	$x \leftarrow$**truncate** $(\sqrt{2}x_n/R)$ $y \leftarrow$**truncate** $(\sqrt{2}y_n/R)$

cells. Unfortunately, the virtual graph produced after the first stage may not be connected. Thus, we need to apply the second stage to obtain a connected graph without crossings of virtual edges.

For the second part, we start testing if we can add a virtual edge to the centroid of those cells (see figure 2) which are second degree neighbors (side neighbors of our side neighbors). If for one of those, we cannot add the virtual edge (i.e. there is no other real node in that cell directly reachable from any real node in current cell) then we try again with those cells being neighbors by side of this particular cell we couldn't find nodes to add the virtual edge. This condition guarantees that the resulting virtual graph will be planar. Figure 5 shows the resulting virtual graph after both stages.



(a) Triangles (b) Squares (c) Hexagons

Fig. 4. First connectivity test. Natural neighbors.

As an example, we give the concrete algorithms used in each stage to add edges to the virtual spanner with an hexagonal tilling. The algorithms for squares and triangles are similar and are not included in here due to space limitations.

The algorithm for the first connectivity test using hexagons is given in algorithm 1..

Algorithm 1. Algorithm for the first stage with hexagons

```
1: procedure ReviewHexagonsStage1(I, t)          ▷ I are the neighbor cells
2:     k ← 0                  ▷ by their side to t, they are enumerated from 0 to 5
3:     while k < 6 do
4:         if isThereEdge(t, I_k) then
5:             addEdge(t, I_k)
6:         end if
7:         k ← k + 1
8:     end while
9: end procedure
```

For the second stage with an hexagonal tilling, all reachable cells which are not side neighbors of the current cell (t) are tested. The test needs to take into account existing virtual links which have been added before, to avoid creating a non-planar virtual spanner. The detailed algorithm is given in 2..

Algorithm 2. Algorithm for the second stage with hexagons

```
1: procedure ReviewHexagonsStage2(I, E, t)       ▷ E are the rest of the cells
2:     k ← 0                          ▷ reachable by t, enumerated from 0 to 11
3:     while k < 6 do                          ▷ Review for the odd cells from E
4:         a ← 2k
5:         b0 ←!isThereEdge(t, I_k)
6:         b1 ←!isThereEdge(I_k, E_a)
7:         b2 ←isThereEdge(t, E_k)
8:         if b0 AND b1 AND b2  then
9:             addEdge(t, E_k)
10:        end if
11:        k ← k + 1
12:    end while
13:
14:    k ← 0
15:    while k < 6 do                         ▷ Review for the even cells from E
16:        a ← (k + 1) mod 6
17:        b ← (2k + 1) mod 6
18:        b0 ←isThereEdge(t, I_k)
19:        b1 ←isThereEdge(I_k, E_b)
20:        b2 ←isThereEdge(t, I_a)
21:        b3 ←isThereEdge(I_a, E_b)
22:        b4 ←isThereEdge(t, E_b)
23:        if !(b0 AND b1) AND !(b2 AND b3) AND b4 then
24:            addEdge(t, E_b)
25:        end if
26:        k ← k + 1
27:    end while
28: end procedure
```

As we stated, the goal of this virtual graph is enhancing the performance of face routing. Thus, we will explain in the next section how real nodes do face routing using the virtual graph, whereas we show the performance enhancements achieved later on.

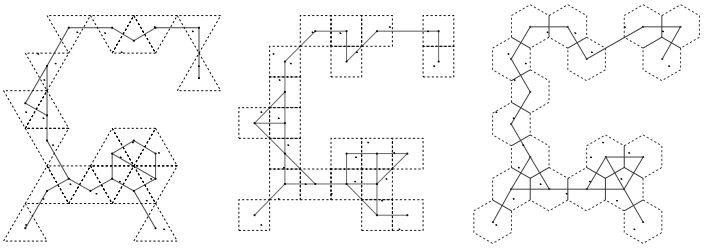
4 Routing with the Virtual Graph

When the protocol enters into face mode, we plan to perform face routing based on the virtual spanner. However, only real nodes can process messages. Thus, we need to understand the two points of view of our proposed scheme. On a high level view we use the virtual nodes whenever a planar graph is needed to forward a message using face routing. In the low level view we always use a real node, which needs to send a message towards another real node, based on its relation with the intended virtual node. We explain how this works based on the Face Routing (FR) algorithm [KSU99]. However, any geographic routing algorithm making use of face routing (i.e. relaying in a planar spanner) can be used as well. For instance, in our experiments we use the GFG variant [BMSU01].

A brief description of the proposed algorithm is presented below. At each step of the algorithm the node currently trying to send the packet to the next neighbor in face mode performs the following operations:

1. Based solely on its coordinates, the node finds out his cell and corresponding virtual node.
2. Using the information from neighbors (obtained by any geographic routing protocol using periodic beacons), the node finds which virtual edges exist according to the procedures explained in the previous section. As we explained before, a virtual edge can only exist to a virtual node if there is a real neighboring node in the corresponding cell.
3. In *face mode* the current real node routing in face mode will use the virtual graph to select (according to face routing) the proper virtual edge to follow. Once it is selected, it uniquely defines the cell that needs to be reached using *real nodes*. The node then sends the packet to any real node in the next cell based on some metric. For instance in our simulations we send the packet to the real node which is more distant to the current real node. If the selected cell is not directly reachable, the real node will greedily hand the packet to another node within the same cell, to reach the target cell.
4. Once a real node in the destination cell (the next cell in the path) received the packet it will forward the packet by repeating the process. Inside a cell the packets can be forwarded greedily because all nodes in a cell a mutually reachable.

The steps above can be used for traversing the face as is depicted in Figure 6. The source node and the target are labeled with 22 and 24 respectively. The source node is in virtual cell $(4, 5)$. Virtual edges exists between $(4, 5)$ and $(3, 5), (3, 4), (4, 4), (4, 6)$. Using the left hand rule node 22 forwards the packet to cell $(3, 4)$ selecting an arbitrary node in such cell. The sequence of virtual nodes, and the sequence of real nodes are depicted in Figure 6.



(a) Triangles (b) Squares (c) Rectangles

Fig. 5. Second test. Reachable neighbors.

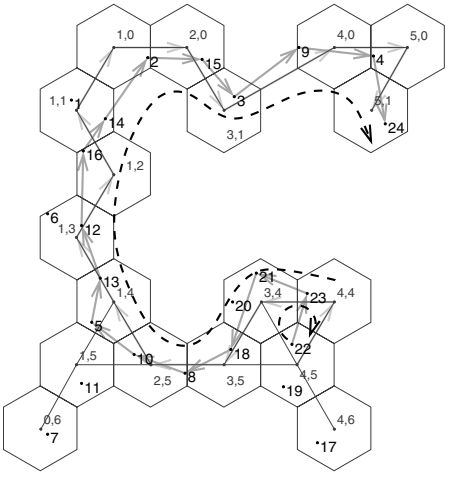


Fig. 6. Face routing in virtual hexagonal graph

5 Experimental Results

In this section we present simulation results to assess the performance of GFG and face routing when run over the different variants of the Virtual Graph. We compare the results with those of the Relative Neighborhood Graph, the Gabriel Graph and the Morelia Graph. We also present real shortest paths computed using Dijkstra's algorithm. Of course, the shortest path cannot be computed using only local information, but provides a good indication of the overall performance of the different proposals.

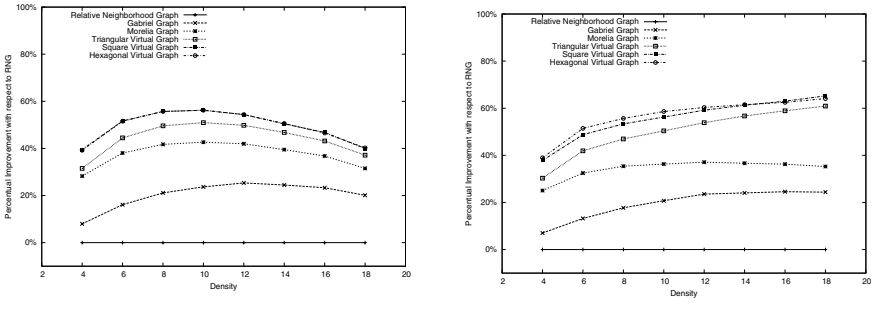
When the protocol enters in face mode, there may be several metrics to decide to which real node within the next cell to send the packet to. In our simulations, we use the euclidean distance, because it is the most common metric used by geographic routing protocols to select neighbors in greedy mode.

5.1 Simulation Setup

We used *connected* random unit disk graphs for our simulations. We test our spanners with different densities, from 4 to 18 with increments of 2. Each one of those densities corresponds to a mean number of neighbors. For each density we used 1000 nodes, which were placed randomly in the simulation area. For each scenario we generated randomly 100 different graphs, so we have obtained 800 graphs for simulation. The size of the simulation area was adapted to preserve the density of the network. Finally, for every graph, we select 1000 different (source,destination) pairs. Thus, each point in the graph represents the average over 100000 routing tasks.

5.2 Simulation Results

We present in this subsection the results of our simulations for different densities of the graphs.



(a) Greedy-Face-Greedy Routing (b) Face Routing

Fig. 7. Efficiency of the Virtual Spanner against three standard spanner test

Figure 7(a) shows the percentual improvement in terms of the mean number of hops required to route from source to destination for different network densities. As we can see in the graph, the higher the density, the better the performance that the proposed protocol achieves, up to a mean density of 10. The reason is that for those mean densities the amount of routing performed in face mode is high. Thus, our proposed virtual spanners allow for a significant reduction in the hop count. The reason being that the virtual spanner manages to use long edges, while traditional plannarization tests (i.e. GG, RNG and MG) remove them. So, the higher the density the more options has the virtual spanner to select best edges. In addition, the increase in density makes traditional tests to remove more (eventually long) edges. As the mean network density goes beyond 10 neighbors per node, we see that our proposed schemes still outperform traditional tests, although the percentual improvement compared to GG and RNG and MG is is reduced. The reason for that reduction is that for those high densities most of the routing is peformed in greedy mode, thus there is no big difference between

approaches. In addition, by having a fixed number of nodes and increasing density means that the overall length of the paths is reduced as density increases. That also affects the reduction in the percentual performance benefit. But, in any case for any density our proposed schemes outperform traditional schemes. For instance, our hexagonal tilling obtains a 40 to 57% improvement compared to RNG for all the ranges of density. The square tilling obtains basically the same results, whereas triangular one has a little bit lower performance, outperforming all of them traditional planarity tests.

To assess the real benefit of the virtual spanner, we performed the same experiments but using only face routing to go from source to destination. As we see in figure 7(b), again a lower density produces longer paths. As before, the reason is that paths become longer because the simulation area is enlarged to accommodate such nodes maintaining the mean density. Figure 7(b) shows that our proposed schemes outperform all other approaches for all densities. In addition, we can see that in this case the gain is higher than with GFG because in this experiment all the routing has been done in face mode regardless of the density of the network.

6 Conclusions and Future Work

We have shown that with the application of the Virtual Graph for representing the underlying structure of a wireless ad-hoc network we can achieve face routing with a fewer number of hops, outperforming in all cases existing techniques (Relative neighborhood graph, Gabriel graph and Morelia graph).

The proposed virtual spanner can be built locally by nodes based solely on local information about neighbors. Thus, it can be perfectly integrated with any geographic routing protocol such as GFG, face routing, etc. Our proposed virtual spanner based on hexagons manages to reduce by a 40 to 60% the number of hops required to route a message from source to destination both for GFG and face routing protocols. This scheme can be integrated with any geographic routing protocol, and can help at improving the performance of such protocols.

For future work, we are working on the use of different routing metrics which may allow the virtual spanner to improve not only the number of hops but energy consumption and quality of the selected paths.

References

[BCG+04] P. Boone, E. Chavez, L. Gleitzky, E. Kranakis, J. Opartny, G. Salazar, and J. Urrutia. Morelia test: Improving the efficiency of the gabriel test and face routing in ad-hoc networks. *Lecture Notes in Computer Science*, 3104:23–24, January 2004.

[BMSU01] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia. Routing with guaranteed delivery in ad-hoc wireless networks. *ACM/Kluwer Wireless Networks*, 7(6):609–616, 2001.

[GS69] K. Gabriel and R. Sokal. A new statistical approach to geographic variation analysis. *Systematic Zoology*, 18:259–278, 1969.

[KSU99] E. Kranakis, H. Singh, and J. Urrutia. Compass routing on geometric networks. In *Proc. 11th Canadian Conference on Computational Geometry*, pages 51–54, Vancouver, August 1999.

[Tou80] G. Toussaint. The relative neighbourhood graph of a finite planar set. *Pattern Recognition*, 12(4):261–268, 1980.

Modified RWGH and Positive Noise Mitigation Schemes for TOA Geolocation in Indoor Multi-hop Wireless Networks

Young Min Ki, Jeong Woo Kim, Sang Rok Kim, and Dong Ku Kim

Yonsei University, Dept. of Electrical and Electronic Engineering
134 Shinchon-Dong, Seodaemun-Gu, Seoul 120-749, Korea
{mellow, c13664, khannury, dkkim}@yonsei.ac.kr
http://mcl.yonsei.ac.kr

Abstract. Time of arrival (TOA) based geolocation schemes for indoor multi-hop environment are investigated and compared to some of conventional geolocation schemes such as least squares (LS) or residual weighting (RWGH). The multi-hop ranging involves positive multi-hop noise as well as non-line of sight (NLOS) and Gaussian measurement noise, so that it is more prone to ranging error than one-hop range. In this paper, RWGH algorithm is modified by adapting weighted residual normalization considering the number of hops taken to measure each ranging. The iterative positive noise mitigation schemes are further developed by using distance enlargement test (DET) to mitigate the multi-hop ranging noise. Simulation results show that the proposed modified RWGH algorithms show 5 to 25% smaller average estimation error compared to LS and RWGH for both positive noise mitigation and no mitigation cases, and the positive noise mitigation schemes provide 28 to 42% error mitigation compared to no mitigation schemes.

1 Introduction

Rather recently, geolocation finding has attracted much attention in the indoor environments. Depending on environments and applications, ranging and geolocation measurements can be performed in a variety of ways, using angle of arrival (AOA), time of arrival (TOA), or Received Signals Strength (RSS) [1]. The TOA technique where range is determined by measured propagation delay between mobile node (MN) and sensor node (SN) is the most popular for accurate geolocation systems [1]. For TOA geolocation, a set of ranging information allow us to draw a multiple number of circles at each SN with radius of their measurement. The traditional geometrical approach for computing the position of MN is to solve for the intersection of the circular lines of position. The circles do not intersect at a point due to the measurement noise, requires more statistically adjustable methods, such as least squares (LS) or residual weighting (RWGH) location estimation [2-3].

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 471–482, 2006.

The traditional geolocation approaches assumed a few fixed, powerful long range nodes, which is similar to base station for communicating with all other nodes in the network. However, if there is no direct communication link between MN and SN, the range must be measured by using multi-hop relaying [4-5]. It was found in [4] that larger number of hops of TOA based ranging makes raging measurement value more unreliable in the system of one-dimensionally placed nodes. This paper assumed the two-dimensional non-linearly arranged multi-hop cases, in which the sum of intermediate range measurements is always greater than the direct distance between source and destination. In this paper, RWGH algorithm is modified by adapting weighted residual normalization considering the number of hops taken to measure each ranging. The iterative positive noise mitigation schemes are further developed by using distance enlargement test (DET) to mitigate the multi-hop ranging noise.

The remainder of the paper is organized as follows. In Section 2, the system description of geolocation problem for multi-hop wireless network is introduced. The Section 3 represents the TOA-based geolocation schemes for one-hop ranging measurements. In Section 4, the proposed geolocation schemes for multi-hop ranging measurements are presented. The performances of the schemes are shown in Section 5. Finally, conclusions are made in Section 6.

2 System Description

2.1 Geolocation in Multi-hop Wireless Network

In wireless indoor network, the nodes have a limited energy supply and a very limited communication range, so that SNs often should route through other wireless nodes to communicate to remote MNs [4-5][8]. Fig. 1 shows a wireless multi-hop network example, where the positions of sensor nodes (SNs) are known but the positions of the remaining mobile nodes (MNs) are unknown. The question is how to get the reliable positions of the MNs by using the known positions

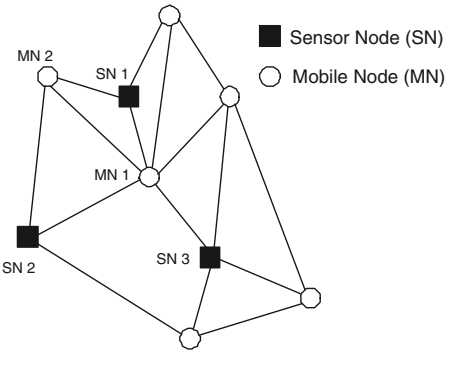


Fig. 1. A wireless multi-hop network example

of SNs. MN 1 can reach to all of three SNs with direct link, while MN 2 has two direct links to SN 1 and SN 2 and one relay link to SN 3 via MN 1. Since at least three ranging measurements are needed for 2-D geolocation, the position of MN 1 can be determined by three direct ranging measurements, but MN 2 has two direct ranging measurements and the third ranging information from SN 3 which is measured by relay link.

2.2 Multi-hop Ranging Measurement

The multi-hop ranging measurement consists of mobile node (MN), sensor node (SN), and R relay nodes (RNs) as shown in Fig. 2. It is assumed that the geolocation systems originally know the locations of SNs and the number of hops between SN to MN, but it does not know location of MN and RN. Therefore, the range measurement between MN and SN should be measured by sum of each hop range measurement. The range measurement between mobile node (MN) and the i-th sensor node (SN) at time instance t is modeled as:

$$r_i(t) = \sum_{j=0}^{R} d_{i,j}(t), \qquad i = 1, 2, ..., N, \tag{1}$$

where $d_{i,j}(t)$ is the range measurement between the $(j-1)$-th relay and the j-th relay node (RN). $d_{i,1}(t)$ is the range measurement between MN to RN 1 and $d_{i,R}(t)$ is the range measurement between RN R to SN, where R is the number of RNs. While the authors of [4-5] assumed the one-dimensional system in which all of nodes are linearly placed, we assume the non-linearly placed multi-hop cases, where sum of intermediate range measurements is always lager than the direct distance between source and destination.

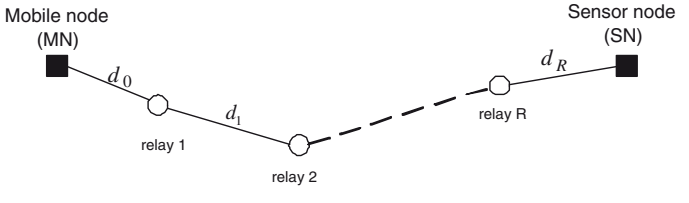


Fig. 2. A ranging example for wireless multi-hop network

2.3 Problem Formulation

The range measurement of the i-th SN is modeled as:

$$r_i(t) = L_i(t) + n_i(t) + NLOS_i(t) + MHR_i(t), \quad i = 1, 2, ..., N, \tag{2}$$

where $L_i(t)$ is the real line of sight (LOS) distance defined as:

$$L_i(t) = \sqrt{(x_M - x_i)^2 + (y_M - y_i)^2}, \tag{3}$$

where (x_M, y_M) and (x_i, y_i) are the coordinates of the MN and the i-th SN respectively. $n_i(t)$ is a measurement noise modeled as zero mean Gaussian random variable. If the variance of one-hop range Gaussian random variable is σ^2, that of R-hop range is $R \cdot \sigma^2$ [4]. When direct LOS path is not detected, $NLOS_i(t)$ for one-hop range can be model as the positive Exponential distribution [2-3][6-7]. Therefore, NLOS error for R-hop range can be modeled as R-Erlang random variable. If multi-hop exists and relay nodes are not linearly placed, $MHR_i(t)$ is positive error. The geolocation problem is to determine the coordinates of the MN (x_M, y_M) by using range measurements of (2).

3 TOA-Based Geolocation Schemes for One-Hop Ranges

3.1 Least Squares (LS)

The LS location estimation fundamentally focuses on minimizing the value of the least square objective function. The LS estimated location is determined as:

$$[\hat{x}_{LS}, \hat{y}_{LS}] = \arg\min_{x,y} \sum_{i=1}^{N} \left(\sqrt{(x - x_i)^2 + (y - y_i)^2} - r_i \right)^2, \tag{4}$$

where (x_i, y_i) is the coordinate of the i-th SN and r_i is the range measurement. N is the number of SN. The square-root term is readily recognized as the distance between a point (x, y) and a SN located at (x_i, y_i). The difference in the parentheses is commonly called *residual* of the estimate [2-3][7].

3.2 Residual Weighting (RWGH)

The residual weighting (RWGH) [2-3] is a form of weighted least-squared algorithm which is a way of mitigating the effects of noise in ranging measurements on NLOS channel conditions. Since NLOS channel conditions introduce strictly positive noise, ranging measurements corrupted by NLOS noise would give location estimates having larger residuals than that of no NLOS case. Therefore, if the number of distance measurements is available, then various sub-groups of range measurements allow us to compute intermediate LS estimates using those sub-groups. Some of these intermediate estimates would have lower residual than the others. The final estimate of the location can be determined as a linear combination of these intermediate estimates weighted by the inverse of its associated residual. Specifically, given N $(N > 3)$ distance measurements, the algorithm calls for the formation of M different distance measurement combinations, where

$$M = \sum_{i=3}^{N} \binom{N}{i}, \tag{5}$$

with each combination being represented by an index set $\{S_k|k = 1, 2, ..., M\}$. For S_k, an intermediate LS estimate $(\hat{x}_k, \hat{y}_k)$ is computed as follows:

$$(\hat{x}_k, \hat{y}_k) = \arg\min_{x,y} R_{es}(x, y, S_k), \tag{6}$$

where the residual of the k-th SN set S_k is defined as:

$$R_{es}(x, y, S_k) = \sum_{i \in S_k} \left(\sqrt{(x - x_i)^2 + (y - y_i)^2} - r_i \right)^2. \tag{7}$$

A normalized residual is computed for every intermediate estimate, $(\hat{x}_k, \hat{y}_k)$ as:

$$\tilde{R}_{es}(\hat{x}_k, \hat{y}_k, S_k) = \frac{R_{es}(\hat{x}_k, \hat{y}_k, S_k)}{\text{size of } S_k}. \tag{8}$$

The final location estimate $(\hat{x}_{RWGH}, \hat{y}_{RWGH})$ can then be computed as:

$$\hat{X}_{RWGH} = \frac{\sum_{k=1}^{M} \hat{X}_k \cdot \left(\tilde{R}_{es}(\hat{x}_k, \hat{y}_k, S_k) \right)^{-1}}{\sum_{k=1}^{M} \left(\tilde{R}_{es}(\hat{x}_k, \hat{y}_k, S_k) \right)^{-1}}, \tag{9}$$

where $\hat{X}_k = [\hat{x}_k \ \hat{y}_k]^T$ and $\hat{X}_{RWGH} = [\hat{x}_{RWGH} \ \hat{y}_{RWGH}]^T$ [2-3].

4 Geolocation Schemes for Multi-hop Ranges

4.1 Modified Residual Weighting (MRWGH)

Since the multi-hop ranging is likely to become inaccurate compared to one of direct path measure, each range measurement should be adopted into location estimation scheme in consideration of its number of hops. RWGH algorithm is modified by adapting weighted residual normalization considering the number of hops taken to measure each ranging, so that larger residual values put with smaller weight into final location estimation. We investigated two versions of modified residual weighting (MRWGH), one of which is given as:

$$\tilde{R}_{es}(\hat{x}_k, \hat{y}_k, S_k) = \frac{R_{es}(\hat{x}_k, \hat{y}_k, S_k)}{\text{size of } S_k} \cdot \prod_{i \in S_k} R_i, \tag{10}$$

where R_i is the number of RNs for the i-th SN to make ranging. The other modified one is given as:

$$\tilde{R}_{es}(\hat{x}_k, \hat{y}_k, S_k) = \frac{R_{es}(\hat{x}_k, \hat{y}_k, S_k)}{\text{size of } S_k} \cdot \sum_{i \in S_k} R_i. \tag{11}$$

Therefore, the modified normalized residual of the k-th SN set S_k having larger number of multi-hop range measurements gives smaller contribution to the final position determined by linear summation of (8) than that of SN set having smaller number of hops.

4.2 Positive Noise Mitigation with Distance Enlargement Test

This paper investigates the multi-hop ranging noise mitigation schemes by using distance enlargement test (DET) [8]. Once the location estimation $(\hat{x}, \hat{y})$ is determined, the distance enlargement test (DET) metric for range measurement of the i-th SN can be computed as:

$$DET_i = r_i - \sqrt{(\hat{x} - x_i)^2 + (\hat{y} - y_i)^2}, \qquad i = 1, 2, ..., N, \tag{12}$$

where r_i is the range measurement and (x_i, y_i) are the coordinates of the MN and the i-th SN. If $|DET_i| \leq \delta$, where δ is the allowable expected error, the location estimation $(\hat{x}, \hat{y})$ is valid. If not, it has some positive ranging noise such as multi-hop ranging noise or NLOS noise [8]. In the latter case, if $DET_i > \delta$, the range measurement has larger positive noise than other ranges. If $DET_i < -\delta$, the range has only Gaussian measurement noise or smaller positive noise than other ranges. We investigate the positive mitigation scheme given as:

$$r_{i,new} = \begin{cases} r_{i,old} - DET_i, & DET_i > \delta \\ r_{i,old}, & otherwise \end{cases}, \qquad i = 1, 2, ..., N, \tag{13}$$

where $r_{i,new}$ is the new range measurement for the i-th SN after positive noise mitigation and $r_{i,old}$ is the old range measurement prior to conduct positive noise mitigation. In our positive noise mitigation scheme, the location estimation such as LS, RWGH and MRWGH is followed by distance enlargement test (DET). Then if positive DET value is present the positive noise is mitigated by (13). Otherwise, noise mitigation is not performed. The location estimation and positive noise mitigation are iteratively performed until DET_i becomes less than δ for all range measurements.

5 Performance Evaluation

5.1 Simulation Setup

The performance of the geolocation algorithms described in Section 3 and 4 is evaluated through simulations. The example of node arrangement is shown in Fig. 3. The regular $L \times L$ grid arrangement of fixed four SNs is assumed and L is set to 30m. One MN and three RNs are uniformly placed in $L \times L$ area and their locations are generated more than 100 times. For each drop, RNs are fixed but MN moves straightly with maximum speed of 8.33m/s. The simulation time for each drop is 20msec, sampling time is set to 200nses, and the MN has a limited communication range of 20m. If SN is within first-hop coverage of the MN, the range measurement of the SN is determined by one-hop range. Otherwise, the range of the SN is measured by multi-hop relaying. The mixed line of sight (LOS)/non-line of sight (NLOS) scenario is simulated using a binomial random variable, such that the channel is likely to be NLOS with probability p, and LOS with probability $(1 - p)$ [3]. Range measurements are generated by adding

measuring noise of Gaussian random variable and NLOS noise of Exponential random variable to the true ranges. The probability density function of NLOS error d (in meters) can be written as:

$$D(d) = \begin{cases} \frac{1}{c \cdot \tau_{rms}} \cdot e^{-\frac{d}{c \cdot \tau_{rms}}}, & d > 0 \\ 0, & otherwise \end{cases}, \tag{14}$$

where c is the speed of light, and τ_{rms} is the delay spread and is set to 30nsec.

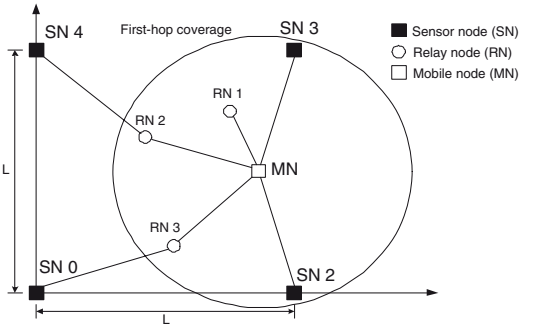


Fig. 3. The basic configuration example for a geolocation system simulation

5.2 Results on LOS Environment

We investigated the LS, RWGH, and two versions of MRWGH: MRWGH1 means the modified version of (10) and MRWGH2 is that of (11). The positive noise mitigation scheme is simulated for each geolocation algorithms in parallel with the simulation of the original algorithms with no mitigation. The positive mitigation threshold δ is set to 0.3m. The performance metric is the average estimation error E_{av}, defined as:

$$E_{av} = E\Big\{ \big| X_M - \hat{X} \big| \Big\}, \tag{15}$$

where X_M and $\hat{X}$ are the actual and estimated locations of a MN. Also, the average number of iterations for mitigation is computed for positive noise mitigated schemes.

Fig. 4 shows the average estimation error as a function of standard deviation of measurement noise in LOS environment. It is shown that MRWGH algorithms show the smallest average estimation error among the simulated schemes, and both versions of MRWGH have little difference in error performance in either no mitigation or mitigation schemes. The average estimation error of MRWGH algorithms is 20 to 25% smaller than that of LS and 9 to 13% smaller than that of original RWGH. It is due to the fact that more uncertain multi-hop ranges give less affects to the final position than one-hop ranges in the MRWGH algorithms. The positive noise mitigated schemes show 28 to 30% smaller error than no

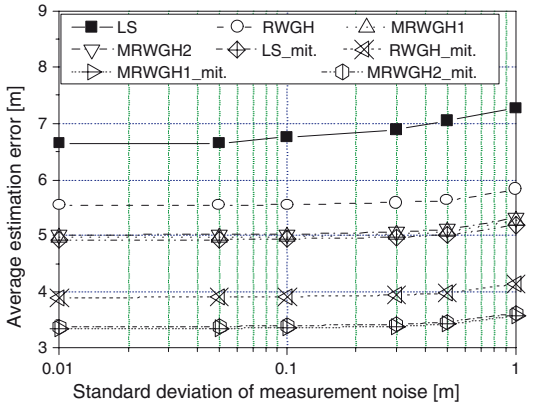


Fig. 4. Average estimation error as a function of standard deviation of measurement noise (LOS case)

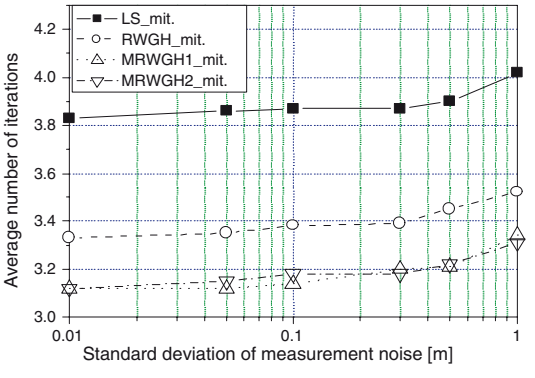


Fig. 5. Average number of iterations for mitigation as a function of standard deviation of measurement noise for positive noise mitigation schemes (LOS case)

mitigation scheme of LS and RWGH, and around 33% less than that of MRWGH algorithms. The RWGH with no mitigation provides almost same estimation error performance as positive error mitigated LS scheme. For all of schemes, the error performance degradation due to measurement noise is within 10%, even though standard deviation of Gaussian noise changes from 0.01m to 1.0m. Fig. 5 represents the average number of iterations for mitigation as a function of standard deviation of measurement noise for positive noise mitigation schemes in LOS case. It is shown that the necessary number of iterations of positive noise mitigation for MRWGH algorithms is around 18% smaller compared to that of LS, and 6% smaller compared to that of RWGH.

5.3 Results on Mixed LOS/NLOS Environment

Fig. 6 shows average estimation error as a function of standard deviation of measurement noise in mixed LOS/NLOS environment where the $p(NLOS)$ is set to 0.2. The average estimation error of MRWGH algorithms is 17 to 22% smaller than that of LS and 5 to 8% smaller than that of original RWGH. The positive noise mitigated schemes show around 37 to 42% smaller error than no mitigation schemes. Since positive noise mitigation schemes manage both NLOS and multi-hop ranging errors, the performance gain in NLOS case is much larger than in LOS case. Fig. 7 represents the average number of iterations for mitigation as a function of standard deviation of measurement noise for positive noise mitigation schemes in mixed LOS/NLOS environment in which the probability of a range

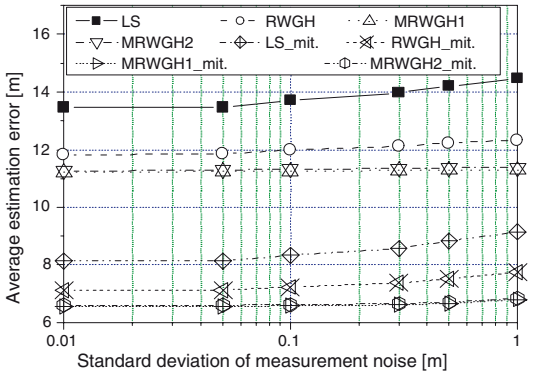


Fig. 6. Average estimation error as a function of standard deviation of measurement noise (mixed LOS/NLOS case, $p(NLOS)$ is 0.2)

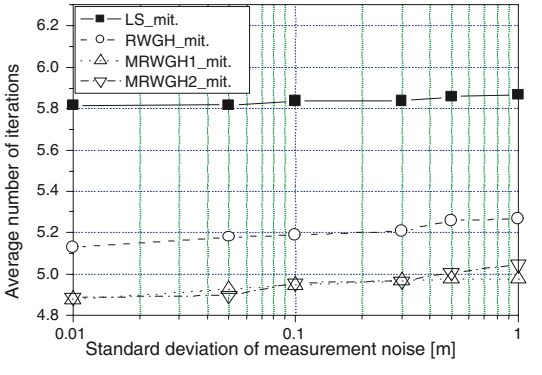


Fig. 7. Average number of iterations for mitigation as a function of standard deviation of measurement noise for positive noise mitigation schemes (mixed LOS/NLOS case, $p(NLOS)$ is 0.2)

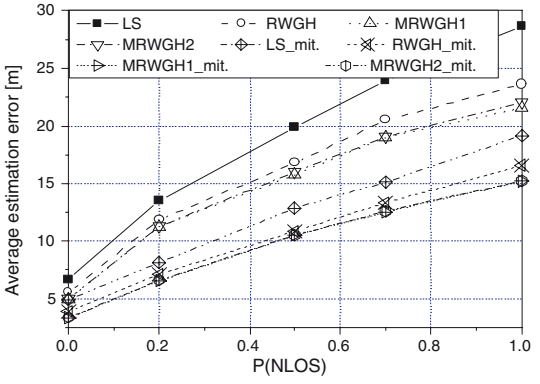


Fig. 8. Average estimation error as a function of $p(NLOS)$ (standard deviation of measurement noise is 0.01)

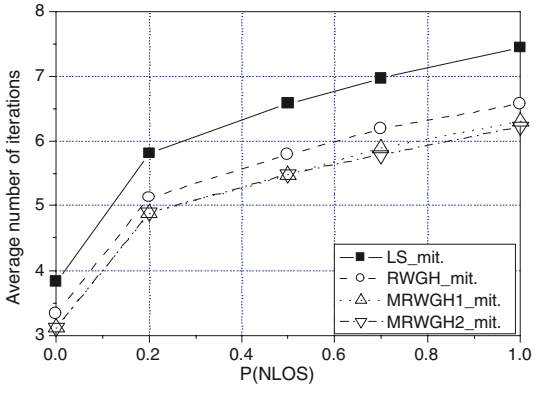


Fig. 9. Average number of iterations for mitigation as a function of $p(NLOS)$ for positive noise mitigation schemes (standard deviation of measurement noise is 0.01)

measurement corrupted by the NLOS noise $p(NLOS)$ is set to 0.2. The number of iterations of positive noise mitigation for MRWGH algorithms is around 17% smaller compared to that of LS, and around 6% smaller compared to that of RWGH.

Fig. 8 represents the average estimation error as a function of $p(NLOS)$ when the standard deviation of measurement noise is 0.01m. It is shown that if the $p(NLOS)$ increases from 0.0 (LOS) to 1.0, the performance difference among the schemes become larger. Since positive noise mitigation schemes could manage both NLOS and multi-hop ranging errors, the performance gain in NLOS case increases when the $p(NLOS)$ becomes larger. Fig. 9 shows the average number of iterations for mitigation as a function of $p(NLOS)$ for positive noise mitigation schemes when the standard deviation of measurement noise is 0.01m. It is

found that the number of iterations of positive noise mitigation for MRWGH algorithms is around 16 to 18% smaller compared to that of LS, and 4 to 6% smaller compared to that of RWGH. It is demonstrated that the MRWGH algorithms improve average estimation error performance compared to the LS and RWGH for both positive noise mitigation and no mitigation cases, and reduce the necessary number of iterations for positive noise mitigation case. Also, the positive noise mitigation schemes provide around 28 to 42% error mitigation effect compared to the no mitigation schemes.

6 Concluding Remarks

The multi-hop ranging often involves positive multi-hop noise as well as NLOS and Gaussian measurement noise, so that it is more prone to ranging error than one-hop range. In this paper, RWGH algorithm was modified by adapting weighted residual normalization considering the number of hops taken to measure each ranging. The iterative positive noise mitigation schemes were further developed by DET to mitigate the multi-hop ranging noise. The proposed schemes were compared to LS and RWGH algorithms in terms of average estimation error and the number of positive noise mitigations. It was demonstrated that the proposed MRWGH algorithms improve average estimation error performance compared to the LS and RWGH for both positive noise mitigation and no mitigation cases, and reduce the necessary number of iterations for positive noise mitigation case. Also, the positive noise mitigation schemes provide around 28 to 42% error mitigation effect compared to the no mitigation schemes.

Acknowledgment

This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment) (IITA-2005-(C1090-0502-0030)).

References

1. Pahlavan K., Li X., Makela J.-P.: Indoor Geolocation Science and Technology. IEEE Communications Magazine, Vol. 40. Issue 2. (2002) 112-118
2. Chen P.-C.: A Non-Line-of-Sight Error Mitigation Algorithm in Location Estimation. IEEE Wireless Communications and Networking Conference (WCNC 1999)
3. Chen P.-C.: A Cellular Based Mobile Location Tracking System. 1999 IEEE 49th Vehicular Technology Conference (VTC 99-Spring)
4. Shi Q., Correal N., Kyperountas S., Niu F.: Perofmrnace Comparison Between TOA Ranging Technologies and RSSI Ranging Technologies for Multi-hop Wireless Networks. 2005 IEEE 62nd Vehicular Technology Conference (VTC 2005-Fall)
5. Shi Q., Kyperountas S., Niu F., Correal N.: Location Estimation in Multi-Hop Wireless Networks. 2004 IEEE International Conference on Communications (ICC 2004)

6. Alavi B., Pahlavan K.: Bandwidth Effect on Distance Error Modeling for Indoor Geolocation. 14th IEEE Personal, Indoor and Mobile Radio Communications (PIMRC 2003)
7. Kannan M., Pahlavan K.: A Comparison of Wireless Geolocation Algorithms in the Indoor Environment. IEEE Wireless Communications and Networking Conference (WCNC 2004)
8. Capkun S., Hubaux J.-P.: Secure positioning of wireless devices with application to sensor networks. 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005)
9. Wylie M.P., Holtzman J.: The non-line of sight problem in mobile location estimation. 1996 5th IEEE International Conference on Universal Personal Communications (ICUPC 96)
10. Chung W.C., Ha D.S.: An accurate ultra wideband (UWB) ranging for precision asset location. 2003 IEEE Conference on Ultra Wideband Systems and Technologies (UWBST 2003)

The Use of Wireless Networks for the Surveillance and Control of Vehicles in an Airport Environment

Augusto Casaca[1], Tiago Silva[1], António Grilo[1], Mário Nunes[1], Franck Presutto[2], and Isabel Rebelo[3]

[1] INESC Inovação, R. Alves Redol 9,
1000-029 Lisboa, Portugal
{Augusto.Casaca, Tiago.Silva, Antonio.Grilo, Mario.Nunes}@inesc.pt
[2] M3 Systems, 1 rue des Oiseaux,
31410 Lavernose-Lacasse, France
Presutto@m3systems.net
[3] ANA, Rua D – Edifício 120, Aeroporto de Lisboa
1802-806 Lisboa, Portugal
Isabel.Rebelo@ana-aeroportos.pt

Abstract. The paper focusses on the use of wireless networks, with special emphasis on Wi-Fi, in the manoeuvering and apron areas of an airport to control the ground vehicles movements in those areas and, consequently, to improve user safety, efficiency of operations and airport security. The use of Wi-Fi for these purposes constitutes a novel approach in an airport environment. Other wireless networks, namely CDMA and Tetra, are also experimented in this project as a lower bit-rate alternative to Wi-Fi. The platform consists of an on-board system in each vehicle, a centralised ground system and wireless networks to allow the communication between the vehicles and ground system. The architecture, protocols and network configurations in use are analysed as well as the respective deployment made in the airport of Porto in Portugal.

1 Introduction

The continuous and steady growth of air traffic leads to an escalating number of accidents and incidents on surface movements. In case of low visibility, since the surveillance and control of movements are based mostly on the "see and be seen" principle, airport stakeholders have little knowledge of ground surface traffic, thus leading to ground movement hazards. In addition, airport congestion is also becoming an increasing problem.

The AIRNET (AIRport NETwork for Mobiles Surveillance and Alerting) project[1] has the high level objectives of improving user safety, efficiency of operations and airport security in the apron and manoeuvering areas of an airport.

The project developed a GPS/EGNOS based low cost platform for the surveillance, control and management of all airport vehicles (eg. catering, luggage, fuel,

[1] The AIRNET project is partially funded by the European Commission in the sixth Framework Program under contract nº 507888.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 483 – 493, 2006.

maintenance, police, firebrigade, etc). These services implement the recommendations of Eurocontrol for A-SMGCS (Advanced Surface Movement Guidance and Control Systems) [1]. The platform consists of an on-board system in each vehicle, a centralised ground station and wireless communication networks to interconnect all the systems [2] [3].

Concerning the wireless communication networks used for this solution the main emphasis is put in the use of Wi-Fi, which is a complete novel approach for these types of applications in an airport environment. In parallel, CDMA and Tetra technologies will also be experimented so that conclusions can be taken on the use of technologies with a lower bit rate than Wi-Fi for the applications envisaged. Finally, for a limited number of situations, a VDL-4 network is also experimented to demonstrate the ability of the AIRNET platform to be compliant with one aeronautical network.

The AIRNET project lasts for three years and is presently running in its last year, in which the AIRNET platform is being deployed in the Porto airport in Portugal, which can be considered a medium sized airport. The platform and the use of the wireless communication networks will be validated by running a complete set of operational scenarios, which have been established by the airport stakeholders. The AIRNET platform is expected to be part of future airport management systems as a building block that can be integrated in A-SMGCS.

In the next section of the paper the AIRNET services will be shortly presented. Section 3 will introduce the AIRNET platform components. Sections 4, 5 and 6 are dedicated to the communication network architecture and to the communication technologies experimented. Section 7 describes the network deployment and finally conclusions are drawn in the last section of the paper.

2 Airnet Services

The AIRNET services will help actors to improve safety for the vehicle movements in the manoeuvering and apron areas of the airport [4]. The AIRNET actors are the Air Traffic Controller (ATCO), the Airport Operation Officer (AOO), the Ground Handling Manager (GHM) and the vehicle drivers.

AIRNET provides four types of services: surveillance, control, guidance and decision support.

The surveillance service dedicated to the ATCO provides continuous surveillance data for the manoeuvering area. The data consists of traffic information on all the aircraft and vehicles in the area and traffic context, which is the airport map representation. The same service is provided to the remaining actors by extending it to the apron area too.

The control service dedicated to the ATCO aims to provide conflict/infringement alerts for the manoeuvering area. It detects conflicts/infrigements on runway caused by aircrafts or vehicles, on taxiway when a vehicle crosses a taxiway while an aircraft is taxing and by incursions in restricted areas. The same service is provided to the

remaining actors, but including the apron area by detecting conflicts betwwen two vehicles or an aircraft and a vehicle.

The guidance service is dedicated to vehicle drivers and includes all the areas of the airport. This service allows drivers to visualize their own positions on a moving map of the airport.

The decision support service is dedicated to the drivers, AOO and GHM. This service aims to provide situation assessment and solutions to optimize the use of vehicles. The decision support service, in concrete, provides real time information about aircrafts, text messages with instructions for the drivers, historical data of the airport and vehicle status information.

3 Airnet Platform

In order to provide the proposed services, the following key enablers are required: human-machine interfaces for the vehicle drivers and ground system users, mobile postioning using GPS/EGNOS, data flow between the vehicles and the central ground system, processing units for running the software applications that provide services to drivers and ground system users.

The AIRNET platform integrates all these enablers and its architecture includes three components: on-board systems, ground system and communication networks. This architecture is shown in Fig. 1.

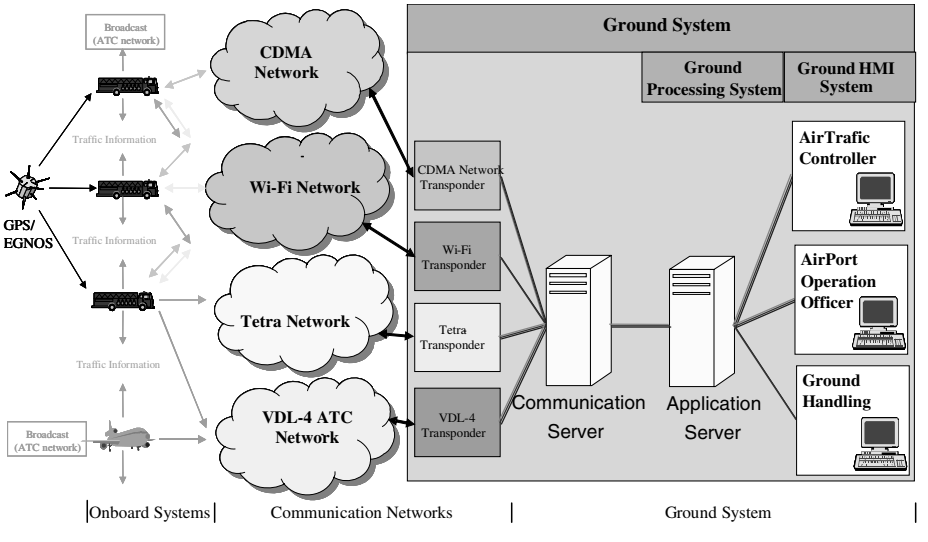


Fig. 1. Architecture of the AIRNET platform

There is one on-board system installed in each vehicle. The system consists of a Communication and Navigation Unit (CNU) and an on-board display for the vehicle driver. The CNU includes a GPS/EGNOS receiver, the wireless communication

network transponders and a PC board. The software modules that implement the AIRNET services on-board run in the PC board. There are five distinct software modules, which are identified according to the services that they provision, namely Traffic Information, Traffic Context, Conflict/Infringement Detection, Service Monitoring (monitors the equipment status) and Decision Support.

The ground system consists of the application server, communication server with the network transponders and a set of monitors for the users of the platform. Software modules equivalent to the ones running in the CNU are running in the application server (ground processing system), namely Traffic Information, Traffic Context, Conflict/Infringement Detection, Service Monitoring and Decision Support. The ATCO, AOO and GHM interact with the platform via the monitors (ground HMI) connected to the application server. The communication server concentrates all the software tasks concerned with the management of the communication links to the on-board systems.

The communication networks allow the exchange of data between the on-board systems and the ground system. They cover the whole maneuvering and apron areas of the airport. Three distinct networks are used for this purpose: Wi-Fi, CDMA and Tetra. The main emphasis of the project is on the use of Wi-Fi, which is a novel approach for an airport maneuvering area environment and, therefore, this network by itself is enough to satisfy all the requirements of the AIRNET platform. However, the project intends also to demonstrate that the platform can also be implemented, although with a lower quality of service, using lower bit-rate communication technologies like CDMA and Tetra. These two networks are commonly found in an airport environment and that is the main reason of their choice as alternative technologies to Wi-Fi. Finally, the VDL-4 network is only used to demonstrate that some of the services can also be implemented in an aeronautical network. The communications server (CS) is the entity responsible for managing the heterogeneity of the wireless communication networks, presenting a common network interface to the ground system services. Like the CNU, its implementation is also based on a PC architecture running the LINUX OS. In the remaining of the paper we only concentrate on Wi-Fi, CDMA and Tetra, which are the networks where all the services can run.

4 Airnet Network Architecture

The detailed AIRNET network architecture is depicted in Fig. 2, where the interconnection to the airport's LAN is also shown. The AIRNET communications are completely based on the IP protocol. The core of the AIRNET network consists of an interconnection VLAN that is separate from the airport LAN where the Airport Operational Management system (AOMS) is located. The Wi-Fi network forms itself an independent VLAN that connects to the AIRNET VLAN.

Within the AIRNET system the details of the communication network are completely transparent to the services. Higher layer software modules, including application modules running on both the CNU and the application server exchange service messages in ASTERIX [5] format without knowing the medium through which the messages will effectively be transmitted. Networking details are dealt with by the Communication Server (CS) in the ground system as referred previously.

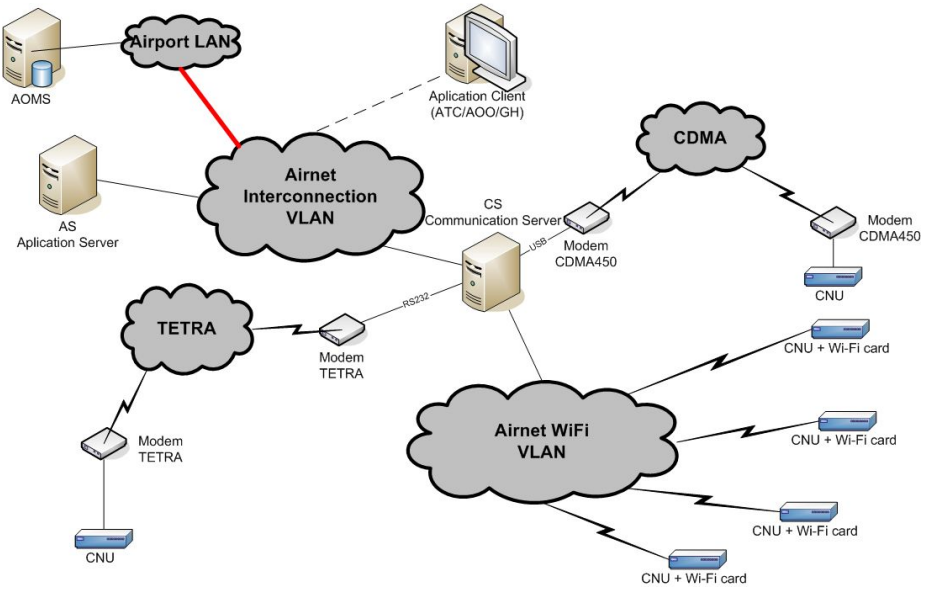


Fig. 2. AIRNET network architecture

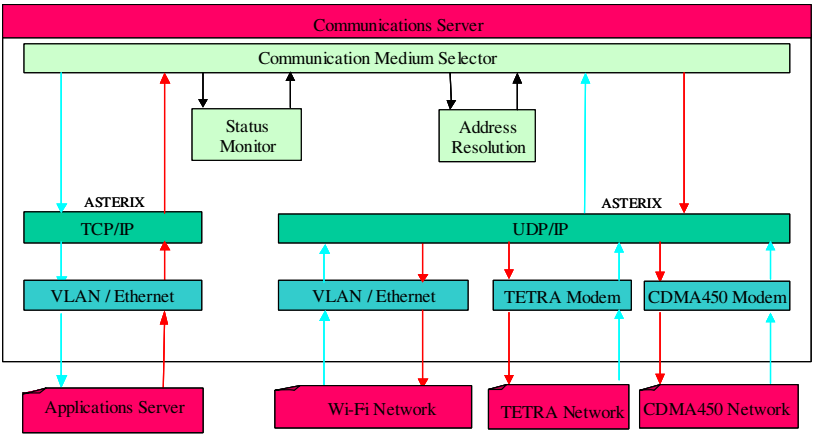


Fig. 3. Architecture of the communication server

Within the CS, the Communication Medium Selector is responsible for the routing decisions, choosing between different wireless technologies. The CNUs and CS are the endpoints of communication from the perspective of the transport layer. Due to the unsuitability of TCP to operate over the air interfaces, communication between the CNUs and the CS is based on the UDP transport protocol. For the services that require stringent delivery guarantees, reliability is implemented at the application layer. Within the cabled network that supports the ground system, TCP is used for added reliability. The gateway between UDP and TCP is located at the communications server.

ASTERIX messages issued by the onboard systems to other onboard systems or to the ground system, as well as messages issued by the application server to the onboard systems are all routed by the CS. Independently of the source, broadcast messages are sent in unicast mode to the CS, which then activates the broadcast mechanisms supported by the target air interface (e.g., broadcast transmission for Wi-Fi and pseudo-broadcast – i.e. multiple unicast – transmission for Tetra and CDMA).

ASTERIX message destinations are uniquely identified by a specific 24-bit Target Address field. Address translation between Target Address codes and UDP/IP addresses is performed at the CS. Another networking function performed by the CS has to do with network transponder status monitoring. The CS periodically checks the status of the network transponders by means of IP-based Ping requests and any failures are readily reported to the general Service Monitoring module at the applicationsserver by means of special ASTERIX messages using a separate TCP port.

The three wireless networks that integrate the AIRNET platform will now be described in greater detail.

5 Tetra and CDMA Networks

5.1 The Tetra Network Architecture

The motivation to test the use of Tetra is that a Tetra network is already deployed at the Porto airport to support voice services and it has the capability of supporting data services too.

The TETRA network is centered on a base station (BS) and supports packet data services with the Specific Connectionless Network Service (S-CLNS). The S-CLNS allows the transmission of IP packets between a TETRA mobile terminal and terminals located in either a fixed IP-based LAN or other mobile terminals using the S-CLNS (see Fig. 4). In AIRNET, the proprietary DIMETRA S-CLNS implementation

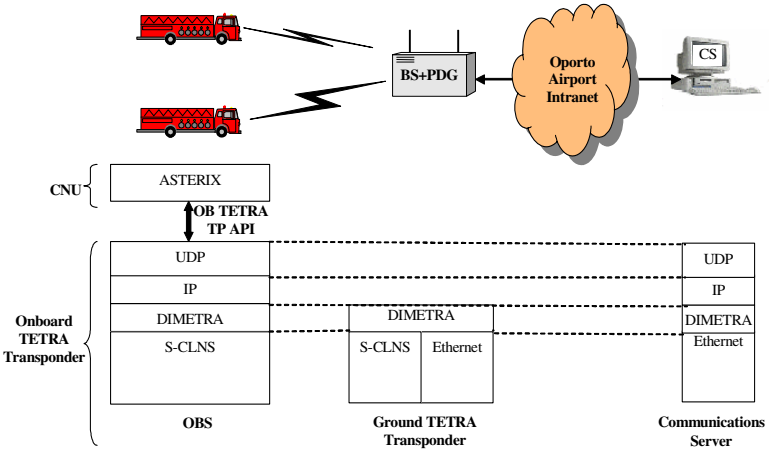


Fig. 4. Architecture of protocols in the Tetra network

is used [6]. The interface with the IP-based LAN is performed by a PC running the Packet Data Gateway (PDG) software. This equipment, together with the BS forms the logical Ground TETRA Transponder when the S-CLNS service is in use. UDP was again chosen as the transport protocol due to the reasons already mentioned for Wi-Fi.

Due to the low bitrate supported by the Tetra technology (maximum of 28.8 kbps per carrier per direction of communication) and the overhead introduced by UDP/IP communication, the AIRNET functionality will be reduced when this technology is used.

5.2 The CDMA Network Architecture

The CDMA network available in Portugal operates in the 450 MHz range. It basically follows the specifications of CDMA2000 defined by 3GPP2, with the physical layer modifications required for use in another frequency band and with lower bandwidth channels (1.25 MHz).

The Portuguese CDMA network operates in two modes: 1xRTT (Radio Transmission Technology) [7] and EV-DO (Evolution, Data Optimized) [8].

In the EV-DO network the maximum bandwidth per sector is 2.4 Mbps downstream and 153.6 Kbps upstream. In the 1xRTT mode the maximum bandwidth per sector and connection is 153.6 Kbps for both downstream and upstream directions. Presently the EV-DO is only available in urban and suburban areas, what fortunately includes the entire AIRNET platform at the Porto airport, requiring, however, that the ground vehicles are equipped with external antennas.

The protocol architecture of the CDMA450 is shown in figure 5.

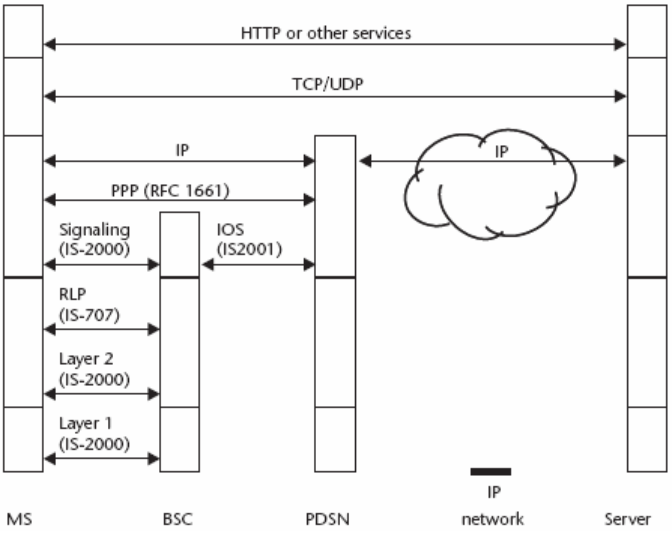


Fig. 5. Architecture of protocols in the CDMA network

On of the advantages of the CDMA protocol architecture is that it is IP based, so its integration with the Airnet network subsystems is seamless and efficient.

Another advantage of CDMA for the Airnet stakeholders is that besides allowing high speed data, this network also provides voice services, both inside the network and also to other public networks, fixed and mobile. Consequently it enables the airport users to establish and receive telephony calls with any telephone user of any network, as well as to access all "normal" telephony call services that mobile telephone users are used to.

Still another important advantage of CDMA450 is that as it operates in a frequency band much lower than UMTS or Wi-FI, it has a much lower attenuation in open air and better coverage in non line-of-sight environments, what means that it can cover a wide area with a single Base Station Controller, making it a possible alternative to support the Airnet services.

6 The Wi-Fi Network Architecture

AIRNET gave special emphasis to the use of Wi-Fi to support the AIRNET services due to its high data rate when compared with other networks, namely Tetra and even CDMA. Besides, Wi-Fi is a private network totally controlled by the airport authorities. This does not happen with CDMA, which is a network under control of a public operator.

In the AIRNET platform the Wi-Fi network is based on the IEEE 802.11a standard [9], which operates in the 5 GHz frequency band, supporting physical bit-rates between 1 Mbps and 54 Mbps. IEEE 802.11a was selected in detriment of its 2.4 GHz counterpart standard IEEE 802.11g [10] due to the fact that the Portuguese communications regulations authority (ANACOM) has authorized the use of higher transmission power in the 5.470-5.725 GHz frequency band for vehicular applications (1 W E.I.R.P versus 100 mW E.I.R.P for the 2.4 GHz frequency band), which greatly reduced the number of APs required to cover the airport.

Among the analysed Wi-Fi architectures, the IP-based Routed-WLAN architecture turned out to be the most advantageous. The Routed-WLAN architecture uses high layer management protocols on top of TCP/IP to configure the network elements: Central Controller and Access Points (AP).

The Central Controller concentrates all the Wi-Fi network "intelligence". Its main responsibilities are:

- Network management services.
- RF channel management.
- AP transmission power management that automatically adapts to interference conditions.
- Handover logic and mobility management.
- Enforcement of security and QoS policies.
- VLAN/VPN management.
- Network monitoring and automatic reconfiguration in response to failure conditions.

The APs have their functionality limited to the PHY and MAC layers, except for the management plane.

In the AIRNET architecture, the APs and the Central Controller belong to a separate VLAN that interconnects to the CS through the interconnection VLAN (see Fig. 2). The main advantages of the selected Routed-WLAN architecture are the following:

- **Security:** Support of IEEE 802.11i [11] features and Virtual Private Networks.
- **Efficiency:** Handover between APs in the same IP subnetwork has a lower latency, since it is processed in the same Central Controller. Authentication is only required the first time that the mobile terminal associates to the WLAN.
- **Compatibility:** Although the full set of advantages provided by the Routed-WLAN requires specific functionality at the APs, any AP can be attached to the network.
- **Scalability:** The Central Controller is the most complex component in the architecture, but it can control hundreds of APs and can be located anywhere in the IP network. Unlike in traditional WLANs the network administrator is able to manage the complete network at this single point, instead of separately configuring each AP.
- **Reliability:** Network redundancy can be easily obtained through the addition of extra Central Controllers that can automatically take control in case of failure of the operating Central Controller. Likewise, in case of failure of one AP, other APs covering the same area can be automatically re-configured to take control of traffic. The Central Controller also implements automatic power control mechanisms to compensate for external interference and/or janmming.
- **Virtualization:** The traffic generated by different airport actors (e.g. ATC, AOO, GHM) can be isolated and separately managed based on network access and utilization policies, including QoS.

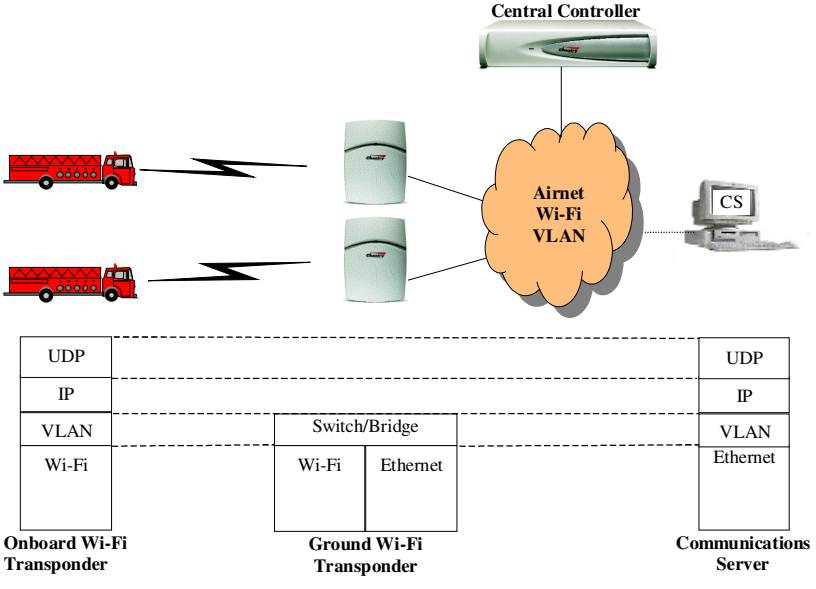


Fig. 6. Architecture of protocols in the Wi-Fi network

7 Deployment

There are currently three deployed wireless networks as part of the AIRNET system: TETRA, CDMA450 and WiFi (802.11a) besides the aeronautical VDL-4 network, which is only used for some services as indicated earlier. Tests on the use of these networks to support the AIRNET services have already started.

The Tetra network covers the entire airport, and most of the airport staff vehicles were already equipped before with Tetra for voice and short message communications. Preliminary results of the data transmission tests in the Tetra network within the AIRNET platform show a limited performance for the AIRNET services. These results point to the need of reducing the number of AIRNET services based on Tetra transmission.

The CDMA network also covers the complete airport area, using ZAPP Telemodem Z010 inside the vehicles, even without external antenna. The airport area is covered in CDMA/1xRTT, and one half of that area is also covered with CDMA/EVDO. Preliminary tests show that CDMA performance is satisfactory for the AIRNET requirements.

The Wi-Fi (IEEE 802.11a) network deployment was intended to assure the complete coverage of the Porto airport apron and manoeuvering areas. The increased transmit power allowed for IEEE 802.11a allowed this goal to be achieved with only 17 APs, which are also able to provide coverage redundancy (see Fig 7).

Fig. 7. Distribution of APs and Wi-Fi (802.11a) coverage at the Porto Airport

Preliminary tests show that on the average, each AP is able to cover from 0 to ~1 Km (vehicle using external antenna and running at 40Km/h), with performance going far beyond AIRNET requirements, which allow future support of other services like, for example, EGNOS broadcast, VoIP (e.g., Wi-Fi Phone) and video streaming,

8 Conclusions

The AIRNET communication networks are already deployed in the Porto airport covering the entire apron and manoeuvering areas. The remaining parts of the

AIRNET platform are also in deployment and initial tests with a limited number of vehicles have started. The tests are part of a set of operational scenarios, which have been defined by the airport stakeholders. They include different pratctical situations, such as, aircraft from landing to stand, aircraft from stand to take-off, runway inspection by the air traffic control service vehicle, conflict on the runway involving a vehicle and an arriving aircraft, conflict in the apron involving a vehicle and an arriving aircraft and ground handling management.

The results obtained until now show the usefulness of the AIRNET services for an efficient control of the airport vehicles and show also that CDMA and Wi-Fi are networks fully capable of supporting this type of applications. Wi-Fi has the advantage that due to its higher data rate can easily support a wider range of new applications in this environment.

References

1. International Civil Aviation Organization, European Manual on Advanced Surface Movement Control and Guidance Systems (A-SMGCS), Doc 9830 AN/452, 2004.
2. Casaca, A., Presutto, F., Rebelo, I., Pestana, G. and Grilo, A., Na airport Network for Mobiles Surveillance, in Proc. of the 16th International Conference on Computer Communications, ISBN 7-121-00308-2, pp. 1703-1708, Beijing, China, 2004.
3. Grilo, A., Nunes, M., Casaca, A., Presutto, F., Rebelo, I., Communication Network Architecture for Mobiles Surveillance in an Airport Environment, Joint International Symposium on Sensors and Systems for Airport Surveillance Proceedings (CDROM), Paris, France, 2005.
4. AIRNET Deliverable D1.1, AIRNET Operational and Systems Requirements, *AIRNET/D1.1/M3S/WP1/OP_SYS_REQ/2.0,* http://www.airnet-project.com/, July 2004.
5. Eurocontrol, "EUROCONTROL Standard Document for Surveillance Data Exchange, Part1: All Purposed Structured Eurocontrol Surveillance Information Exchange (ASTERIX)", v 1.29, February 2002.
6. Motorola, "DIMETRA Packet Data Service – Programmer's Guide", Release 3.1, March 2000.
7. S. Agrawal, I. Acharya, S. Goel, "Inside 3G Wireless Systems: The 1xEV-DV Technology"; TATA Consulting Services, March 2003
8. Lawrence Harte, "Introduction to EVDO, Physical Channels, Logical Channels, Network and Operation"; Althos Publishing, 2004
9. IEEE 802.11a, "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band", IEEE, 2003.
10. IEEE 802.11g, "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY), Specifications: Higher-speed Physical Layer (PHY) Extension to IEEE 802.11b", IEEE, 2003.
11. IEEE 802.11i, "Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements", Draft version 10, IEEE, 2004.

Security Analysis and Implementation Leveraging Globally Networked RFIDs

Namje Park[1,2], Seungjoo Kim[2], Dongho Won[2,*], and Howon Kim[1]

[1] Information Security Research Division, ETRI,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{namjepark, khw}@etri.re.kr
[2] Information Security Group, Sungkyunkwan University,
300 Cheoncheon-dong, Jangan-gu, Suwon, Gyeonggi-do, 440-746, Korea
{njpark, skim, dhwon}@security.re.kr
http://www.security.re.kr

Abstract. Mobile RFID (Radio Frequency Identification) is a new application to use mobile phone as RFID reader with a wireless technology and provides new valuable services to user by integrating RFID and ubiquitous sensor network infrastructure with mobile communication and wireless internet. However, there are an increasing number of concerns, and even some resistances, related to consumer tracking and profiling using RFID technology. Therefore, in this paper, we describe the security analysis and implementation leveraging globally networked mobile RFID service which complies with the Korea's mobile RFID forum standard.

1 Introduction

RFID is recognized as the key technology for ubiquitous network which refers to an environment where information can be acquired at anytime and anywhere through network access [10]. RFID technologies consider the environment in which RFID tags are mobile and RFID readers are stationary. On the other hand, in future RFID technologies could consider the environment in which RFID tags are stationary and readers are mobile. RFID based on mobile telecommunications services can be the best example of this kind of usage. RFID based mobile telecommunications services could be defined as services which provide information access through the telecommunication network by reading RFID tags on some objects with a RFID reader in mobile terminals such as cell phones. RFID tags play an important role as a bridge between offline objects and online information. The RFID enabled cell phone was already introduced by Nokia in 2004.

The future RFID tags will be evolved as active tags which have networking capabilities and will be a key component of the ubiquitous network environment rather than current passive RFID tags. In this stage, RFID tags will need network addresses

* Dongho Won is the corresponding author for this paper. The third author of the research was supported by the University IT Research Center Project funded by the Korean Ministry of Information and Communication.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 494 – 505, 2006.

for communications. For the ubiquitous network, current RFID related technologies need to be changed to reflect the features of mobile telecommunications services. Also, additional technologies for RFID based mobile telecommunications services should be established to provide harmonized operation of services.

A new security technology is required to provide safe service among mobile RFID tag, terminal, and application to minimize the threat of personal information infringement and leakage as the threat of personal information protection infringement increased due to the mobility of mobile RFID reader, the information leakage due to mobile communication and wireless internet environment is expected, the mobile RFID service can be used illegally and RFID tag information can possibly be counterfeited or falsified. Therefore, in this paper, we describe the security analysis and implementation leveraging globally networked mobile RFID service which complies with the Korea's mobile RFID forum standard. This is new technology to RFID will provide a solution to protecting absolute confidentiality from basic tags to user's privacy information.

2 Networked Mobile RFID Services

Networked RFID means an expanded RFID network and communication scope to communicate with a series of networks, inter-networks and globally distributed application systems. So it makes global communication relationships triggered by RFID, for such applications as B2B, B2C, B2B2C, G2C, etc.

Mobile RFID loads a compact RFID reader in cellular phone, providing diverse services through mobile telecommunications networks when reading RFID tags through a cellular phone. Since the provision of these services was first attempted in Korea, their standardization has been ongoing since 2005. Korea's mobile RFID technology is focusing on the UHF range (860~960MHz), since UHF (Ultrahigh Frequency) range may enable longer reading range and moderate data rates as well as relatively small tag size and cost. Then, as a kind of handheld RFID reader, in the selected service domain the UHF RFID phone device can be used for providing object information directly to end-user using the same UHF RFID tags which have spread widely.

Mobile RFID service is defined as to provide personalized secure services such as searching the products information, purchasing, verifying, and paying for the products while on the move through the wireless internet network by building the RFID reader chip into the mobile terminal [1,2,4]. The service infrastructure required for providing such RFID based mobile service is composed of RFID reader, handset, communication network, network protocol, information protection, application server, RFID code interpretation, and contents development, and the configuration map is as follows.

Mobile RFID service structure is defined to support ISO/IEC 18000-6 A/B/C through the wireless access communication between the tag and the reader, however there is no RFID reader chip supporting all three wireless connection access specifications yet that the communication specification for the mobile phone will be determined by the mobile communication companies. It will be also possible to mount the RF wireless communication function to the Reader Chip using SDR (Software Defined Radio) technology and develop ISO/IEC 18000-6 A/B/C communication protocol in software to choose from protocols when needed.

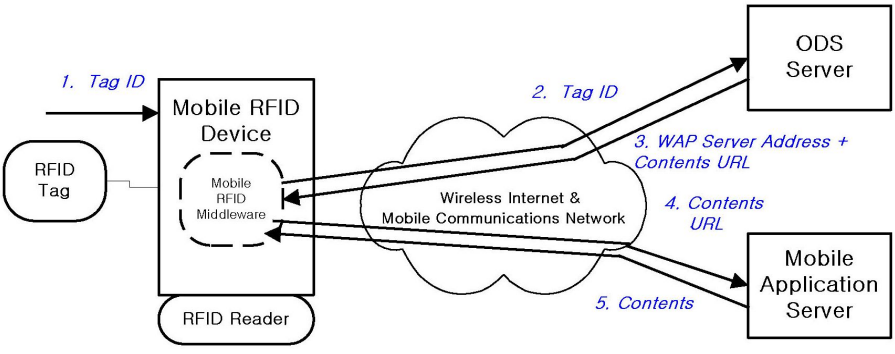


Fig. 1. Basic Communication Model for Mobile RFID Services

Mobile RFID network function is concerned with the communication protocols such as the ODS (Object Directory Service) communication for code interpretation, the message transportation for the transmission and reception of contents between the mobile phone terminal and the application server, contents negotiation that supports mobile RFID service environment and ensures the optimum contents transfer between the mobile phone terminal and the application server, and session management that enables the application to create and manage required status information while transmitting the message and the WIPI (Wireless Internet Platform for Interoperability) extended specification which supports these communication services [2,9,12,14].

The service model, as shown in figure 1, consists of tag, reader, middleware system, and information server. In the point of view of information protection, the serious problem for the RFID service is a threat of privacy [3,5,12]. Here, the damage of privacy is of exposing the information stored in tag and the leakage of information includes all data of the personal possessing the tag, tagged products and location. The privacy protection on RFID system can be considered in two points of view. One is the privacy protection between the tag and the reader, which takes advantage of ID encryption, prevention of location tracking and the countermeasure of tag being forged. The other is of the exposure of what the information server contains along with tagged items [6,7,8]. First of all, we will have a look about the exposure of information caused between tag and reader, and then discuss about the solution proposing on this paper.

3 Mobile RFID-Oriented Security Threats and Requirements

3.1 Some Mobile RFID-Oriented Security Threats

Mobile RFID-oriented security threats are summarized [9,12]. Firstly, RFID tag identifier, ID, can be easily eavesdropped by intercepting broadcasted radio signals or by actively reading RFID tag. Accordingly, it is possible to track RFID-tagged object or monitor the user carrying a specified tag ID using invisible rogue RFID reader. Secondly, RFID tag can contain some important data such as passwords, IDs, user

specific service data for application, etc. Thus, unauthorized tag access can cause denial or misused of service such as a permanent disablement of tag or illegal modification of tag-stored data. Thirdly, Whenever a RFID reader reads a tag ID, its historical reading record like location and time can be collected without agreement of tag user. In especial, if the application of tag is tightly coupled with people, this can cause the violation of privacy due to leakage of the collected historical context data such as the user's preference profile. Finally, Mobile RFID applications need more strict adult verification. Currently teenagers and even elementary school students below 10 are using cell phones which are a ubiquitous information terminal and must be a private device. So they can access adult contents very easily. A strict and elaborate mechanism for adult verification should be provided to protect young people from adult contents. But currently the adult verification is provided within contents at the application layer. That is, the control role is given to contents providers, which means network operators called ISPs cannot control illegal behaviours providing adult contents.

3.2 Security Requirements for Secure Mobile RFID Services

Mobile RFID service structure provides its services by associating the mobile communication network and the RFID application service network based on the RFID tag. The area to consider the security basically is the RFID tag, reader terminal area, mobile communication network area, RFID application service network area, and security issues like the confidentiality/integrity/authentication/permission /non-repudiation shall be considered in each network area. Especially, as the mobile RFID service is the end user service, the issue of privacy protection must inevitably become a serious issue to consider, and as the contents accessibility increases due to the off-line hypertext property of RFID, the authentication for adult service must also become another important issue to consider.

1) Mobile RFID service based on the user's ownership of tagged products needs to guarantee the confidentiality on the tag code information or user data information for personal privacy protection. In this case, mobile RFID application service provider shall provide the confidentiality to the said information or other means to prevent personal privacy infringement.
2) The integrity of the data shall be guaranteed in order to check counterfeiting/falsification of the data transmitted through the communication path in each section of the mobile RFID service network reference structure. However additional code based data integrity other than the least method (for example, CRC) specified in the air interface specification is not required in the communication section between tag and reader terminal considering the limit of the calculation capacity of the tag. However, it is necessary to develop a method to secure the data integrity in the tag for special mobile RFID application service where the personal information is stored in the user data information of the tag and transmitted.
3) The authentication in the mobile RFID can be divided into the device authentication in each network layer and the service user authentication.
   - Device Authentication: Device authentication refers to the authentication of the RFID reader mounted to cellular phone, and mobile RFID service requires the

device authentication as it is based on the inter-working service between heterogenous networks (mobile communication network - RFID application service network).
- User Authentication: User authentication refers to the authentication for mobile RFID service users, and the user authentication is generally required for the reader terminal to access the application server to obtain mobile RFID service contents.

4) The authentication that must be considered in the mobile RFID service structure is as follows.
   - Tag Access Control: Reader terminal can give various commands to the tag, and the tag shall be able to support the access authentication through password especially when executing sensitive commands such as write/delete/lock/kill.
   - Reader Execution Authorization: Refers to the function that verifies whether the user is valid for executing sensitive reader commands such as write/delete/lock/kill at the reader terminal, and it can be possible to develop the reader execution authorization in developing the reader terminal.
   - Authorization for Adult Service: The authorization for adult service is required as the adult content provided by mobile RFID service can be accessed indiscreetly.
   - User Authorization: Must provide the access control for each user or the access object in case of providing different services to each user accessing the application server or differentiating the access level per user.
5) Mobile RFID application service including the processes like bill payment between the reader terminal user and the application server requires the non-repudiation for the data transmitted by the reader terminal user and the application server. In this case, the reader terminal and the application server must be able to execute non-repudiation.
6) Mobile RFID application service that uses the password for halting the tag or authorizing the access to the tag shall be able to safely manage such passwords and safely authorize the key to the reader terminal, and such functions shall be provided by the mobile RFID service infrastructure; for example, the application server or separate key management server.
7) Since mobile RFID service is a B2C service using RFID tag for end users, it inevitably accompanies the issues of personal privacy infringement that it must provide solutions for such issues. The personal privacy issue shall consider both the location privacy relating to the personal identifier role of the RFID tag and the information privacy relating to the identification of personal belongings by browsing the tag interface information through the interpretation of the and the tag code.

4 Key Technology and Solution

4.1 Overview of Secure Networked Mobile RFID Environment

The mobile RFID is a technology for developing a RFID reader embedded in a mobile terminal and providing various application services over wireless networks.

Various security issues - Interdomain security, privacy, authentication, E2E (End-to-End) security, and untraceability etc. - need to be addressed before the widespread use of mobile RFID. Model of mobile RFID service as shown in figure 2 defines additional three entities and two relationships compared to that defined in RFID tag, RFID access network, RFID reader, relation between RFID tag and RFID reader, relation between RFID reader and application server.

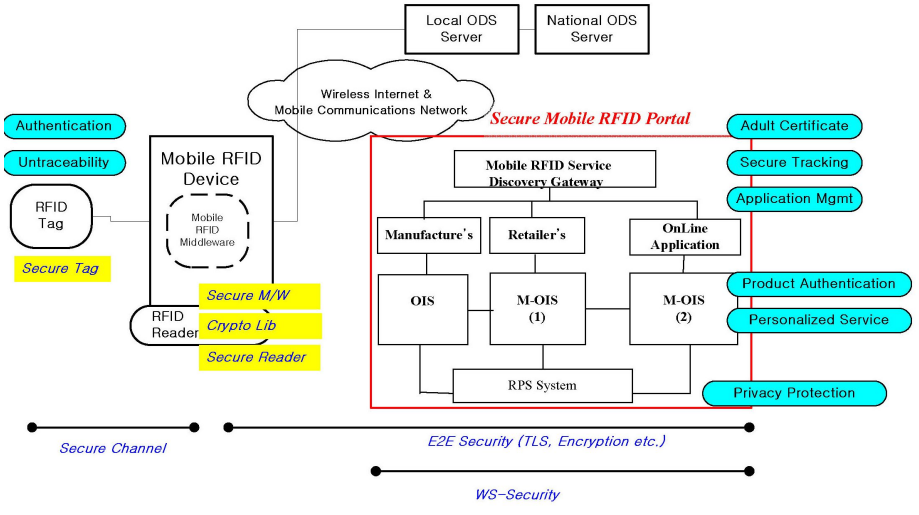


Fig. 2. Conceptual Architecture for Secure RFID over Mobile Networks

Generally, in mobile RFID application such as smart poster, Application Service Provider (ASP) has the ownership of RFID tags. Thus, mobile RFID users have to subscribe to both the ASP for these kinds of RFID services and mobile network operator for mobile communication service. Namely, there exist three potentially distrusted parties: user owned RFID reader, mobile network operator, and ASP. Accordingly, trust relationship among three parties must be established to realize secure mobile RFID service. Especially, when a RFID reader tries to read or change RFID service data stored in tag, the reader needs to get a tag access rights. Additionally, it is important that new tag access rights whenever some readers access a same tag must be different from the already accessed old one.

MRF-Sec 631 strategy represents 6 standard security functions at mobile RFID middleware, 3 major security service mechanisms using 6 security functions, and 1 secure mobile RFID application portal service in order to realize the above 3 security service mechanisms. What is the MRF-Sec 631 strategy? 6-standards security functions are mobile RFID Data encryption API function, mobile RFID secure communication API function, mobile RFID password management API function, EPC C1G2 security command API function, adult certification API function, and privacy protection API function. 3-security service mechanisms are authentication service

mechanism, privacy protection service mechanism, and secure location tracking service mechanism. 1-secure application service is secure mobile RFID application portal service.

4.2 Security Enhanced Mobile RFID Middleware in the Mobile Phone

One of the key problems of the mobile RFID technology is how to quickly use the mobile RFID reader and how to integrate it with the application software installed in the mobile device. In the face of numerous different existing application software, developing a independent mobile RFID middleware layer is a good idea. The mobile RFID middleware layer is in the middle of the RFID reader and the application logic layer. The mobile RFID middleware layer will manage the RFID readers and server for the application logic layer. So the application logic layer based mobile RFID technology can focus on implementing commerce logic.

WIPI is required to come into force on in Korea in case of mobile phone as from 2005 to support interoperability platform for various application software and hardware platform [2]. Therefore we chose WIPI for basic software development platform of mobile phone and the software architecture and the relation between each software functions are shown as figure 3. The software architecture is composed of REX OS, WIPI HAL API, WIPI Runtime Engine, WIPI C API, phone application, Browser parser, and phone GUI. Most functions for mobile RFID technology are designed in the WIPI C API and they are Reader Control, Tag Control, Buffer Control and Filter Control for interfacing with RFID reader and Code Decoder, URN (Uniform Resource Name) Converter, FQDN (Fully Qualified Domain Name) Converter, DNS Resolver and connect Contents Server for communicating with a local ODS server and the contents web server.

In the WIPI specification, the core functions are the functions of handset hardware, native system software, handset adaptation module, run time engine, APIs, and application programs are the areas of the core functional specifications of WIPI. Actually, in the WIPI specifications, only the handset adaptation and APIs are included and the other parts of functions of the wireless Internet platform are considered as the requirements to the handset vendors whether they accept it or not. For example, the run time engine part is required as the mode of download of binary code for its maximum performance.

The core functions of the WIPI are the handset adaptation and APIs which are called 'Handset Adaptation Layer (HAL)' and 'Application Adaptation Layer (AAL)', respectively. The HAL defines an abstract specification layer to support hardware platform independence when porting applications. The AAL defines the specifications for API of the wireless Internet platform. The AAL support the C/C++ and Java programming languages.

Mobile RFID middleware is implemented by extending WIPI platform to provide RF code related information obtained from RF tag through RFID reader attached on mobile phone. Functions of RFID WIPI C API [13] include RFID Reader Control, Buffer Control, Tag Control, Filtering, and Networking for Code decoding, URN conversion, FQDN conversion, DNS resolving and Contents service. WIPI Runtime Engine software for mobile RFID functions is extended to support RFID WIPI C API [11,13] and RFID HAL API. Functions of RFID HAL API include RFID reader

control, Buffer control, Tag control, Filtering, Networking for configuring IP address of Local ODS server. Figure 3 shows middleware functions and software

The RFID device handler provides the definitions for functions of starting the platform and transferring the events from the upper layer of HAL to the RFID H/W Reader. The categories of RFID device handler API cover call, RFID device, network, serial communication, short message service, sound, time, code conversion, file system, input method, font, frame buffer, and virtual key. The AAL provides the definitions for functions of adaptive functions for RFID engine, C/Java API, crypto libraries, and RFID security components.

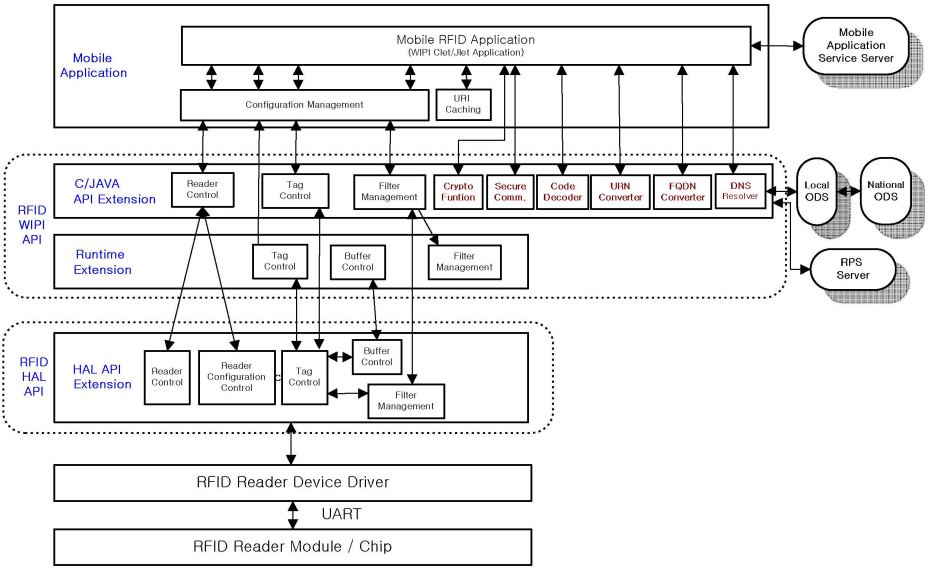


Fig. 3. Security Enhanced Mobile RFID Middleware in the Phone

4.3 Mobile RFID Privacy Protection Service System

Widespread deployment of RFID technology may create new threats to privacy due to the automated tracking capability. Especially, in the mobile RFID environment, privacy problem is more serious since RFID reader is contained in handheld device and many application services are based on Business-to-Costumer model. The RPS (RFID user Privacy management Service) provides mobile RFID users with information privacy protection service for personalized tag under mobile RFID environment [4,8,9]. When a mobile RFID user possesses an RFID tagged product, RPS enables the owner to control his backend information connected with the tag such as product information, distribution information, owner's personal information and so on.

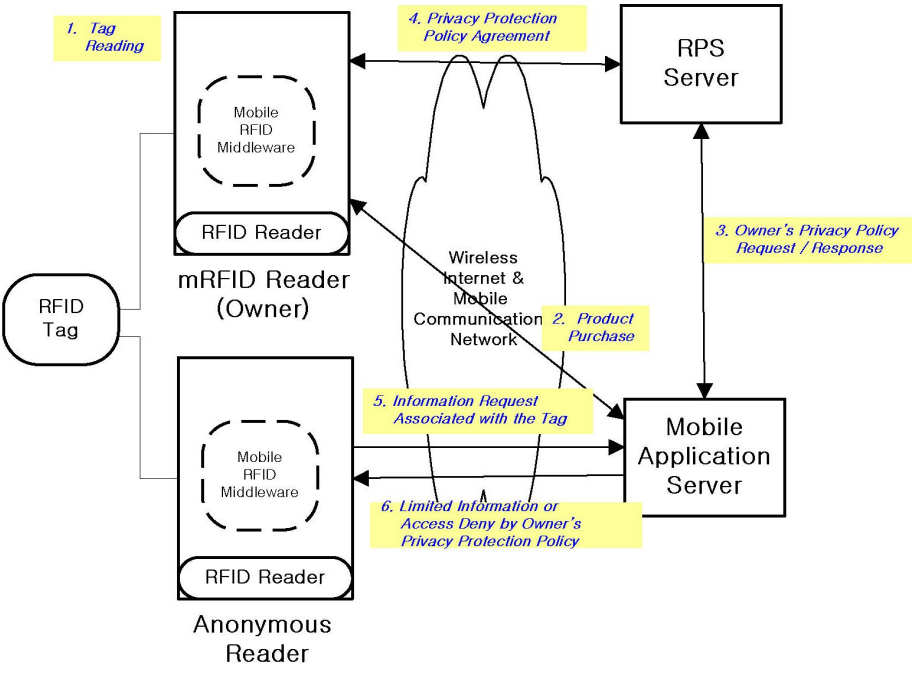


Fig. 4. Service Scenario of RPS Services

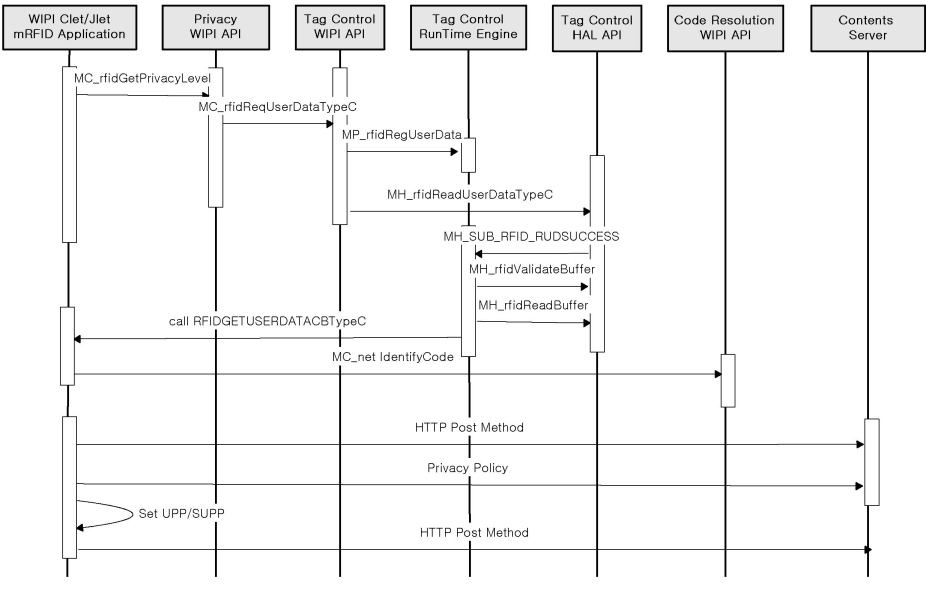


Fig. 5. Procedure of RPS Services

Main features of this service mechanism are owner's privacy protection policy establishment and management, access control for information associated with personalized tag by owner's privacy policy, obligation result notification service, and privacy audit service by audit log management. The brief personal privacy protection process using above functions of RPS is as follows.

Firstly, mobile RFID reader reads the Tag ID and obtains the network addresses of various information such as the product information integrated to the Tag ID through ODS resolver process. Secondly, requests the application server the product information connected to Tag ID. Thirdly, application receives the personal privacy protection policy in relation to the product information through RPS. Finally, the product information is protected appropriately for the privacy protection policy configured by the individual and sent to the reader. The information connected to the Tag ID reflecting personal privacy protection policy through above process is circulated through the network, and it is expected to solve the personal privacy infringement issue through RFID network infrastructure.

4.4 Portal Service System for Secure Mobile RFID Application

Secure mobile RFID application portal is a secure service portal for various mobile RFID application services. The service provider using SMAP (Secure Mobile Application Portal) can easily deploy several mobile RFID applications guaranteed with security and privacy protection.

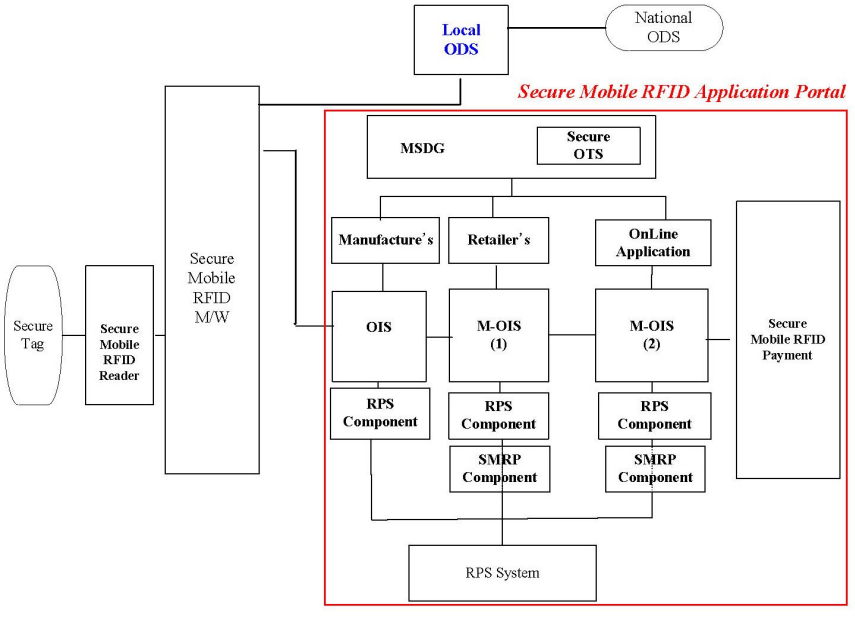


Fig. 6. Architecture of Secure Mobile RFID Application Portal Service

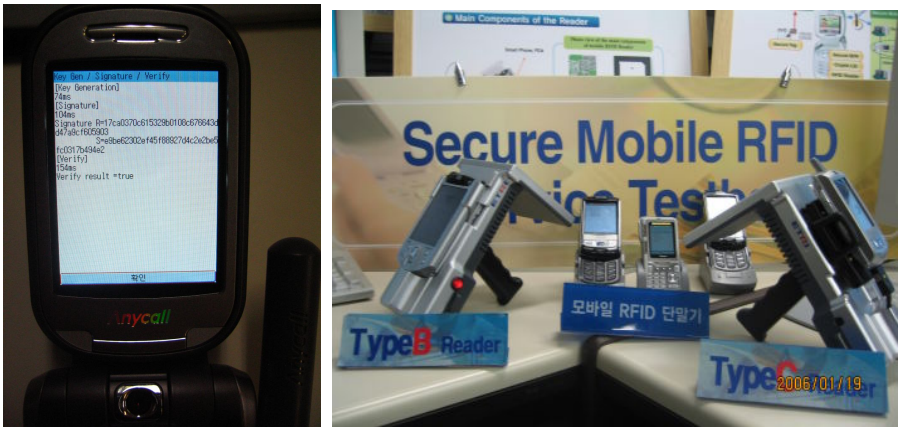


Fig. 7. UHF 900Mhz Mobile RFID Phone Reader

Main features of secure mobile RFID application portal service platform are mobile RFID service discovery, secure object traceability service, application information service, mobile OIS (Object Information Server) generation & management service, mobile RFID privacy protection service, mobile RFID payment service, and mobile RFID security mechanisms - Authentication/Privacy/Untraceability.

5 Conclusion

As mentioned above, mobile RFID is a newly promising application using RFID technology. However, mobility of reader and its service model that is different from RFID service in retail and supply chain will cause some additional security threats.

In this paper, we tried to introduce the concept of mobile RFID and expose some additional security threats caused by it. The frequency band to support the air protocol is allocated at 908.5MHz to 914MHz by TTA (Telecommunication Technology Association) in Korea to comply with ISO 18000-6 for air interface communications at 860MHz to 960MHz. And we describe a way to incorporate its new technology to work with cell phones in particular as an external security reading device (replacing 900MHz) and same time as an added security service to manage all RFID mobile device mediums. With this purpose, the application areas of this service platform are also briefly presented. By doing so, the customized security and privacy protection can be achieved. In this regard, the suggested technique is an effective solution for security and privacy protection in a networked mobile RFID system.

References

1. Tsuji T. Kouno S. Noguchi J. Iguchi M. Misu N. and Kawamura M.: Asset management solution based on RFID. NEC Journal of Advanced Technology. Vol.1, No.3, Summer. (2004) 188-193

2. Jongsuk Chae, Sewon Oh: Information Report on Mobile RFID in Korea. ISO/IEC JTC 1/SC 31/WG 4 N 0922, Information paper, ISO/IEC JTC 1 SC 31 WG4 SG 5 (2005)
3. Seunghun Jin, et. al.: Cluster-based Trust Evaluation Scheme in Ad Hoc Network. ETRI Journal, Vol.27, No.4 (2005) 465-468
4. S. E. Sarma, S. A. Weis, and D.W. Engels: RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT (2002)
5. Wonkyu Choi, et. al.: An RFID Tag Using a Planar Inverted-F Antenna Capable of Being Stuck to Metallic Objects. ETRI Journal, Vol.28, No.2 (2006) 216-218
6. Weis, S. et al.: Security and Privacy Aspects of Low-Cost Radio Frequency identification Systems. First International Conference on Security in Pervasive Computing (SPC) 2003
7. M. Ohkubo, K. Suzuki and S. Kinoshita: Cryptographic Approach to "Privacy-Friendly" Tags. RFID Privacy Workshop (2003)
8. Jiwoon Ahn, et. al.: An Analysis of Consumer Preferences among Wireless LAN and Mobile Internet Services. ETRI Journal, Vol.28, No.2 (2006) 205-215
9. Wung Park, Byoungnam Lee: Proposal for participating in the Correspondence Group on RFID in ITU-T. Information Paper. ASTAP Forum (2004)
10. Sangkeun Yoo: Mobile RFID Activities in Korea. The APT Standardization Program (2006)
11. Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim: WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment. Lecture Notes in Computer Science, Vol. 3842. Springer-Verlag (2006) 741–748
12. Byungho Chug, et. al.: Proposal for the study on a security framework for mobile RFID applications as a new work item on mobile security. ITU-T, COM17D116E, Geneva (2005)
13. MRF Forum: WIPI C API Standard for Mobile RFID Reader (2005)
14. MRF Forum: WIPI Network APIs for Mobile RFID Services (2005)

Smart Blood Bag Management System in a Hospital Environment

Soo-Jung Kim[1, 3], Sun K. Yoo[2, 3], Hyun-Ok Kim[4], Ha-Suk Bae[5], Jung-Jin Park[6, 7], Kuk-Jin Seo[1, 9], Byung-Chul Chang[8]

[1] Graduate School of Biomedical Engineering, Yonsei Univ. 134 Shinchon-dong Seodaemun-ku Seoul, Korea
[2] Dept. of Medical Engineering, Yonsei Univ. College of Medicine, 134 Shinchon-dong Seodaemun-ku, Seoul, Korea, Correspondence
sunkyoo@yumc.yonsei.ac.kr
[3] Center for Emergency Medical Informatics, 134 Shinchon-dong Seodaemun-ku, Seoul, Korea
[4] Dept. of Laboratory Medicine, Yonsei Univ. College of Medicine, 134 Shinchon-dong Seodaemun-ku, Seoul, Korea
[5] Dept. of Rehabilitation Medicine, Ewha Womans Univ. College of Medicine, 911-1 Mok-dong Yangchun-ku, Seoul, Korea
[6] Graduate School of Information, Yonsei Univ. 134 Shinchon-dong Seodaemun-ku Seoul, Korea
[7] Center for Signal Processing Research, Yonsei Univ. 134 Shinchon-dong, Seodaemun-ku, Seoul, Korea
[8] Dept. of Thoracic & Cardiovascular Surgery, Yonsei Univ. College of Medicine, 134 Shinchon-dong Seodaemun-ku, Seoul, Korea
[9] Human Identification Research Center, Yonsei Univ. 134 Shinchon-dong Seodaemun-ku, Seoul, Korea

Abstract. In order to provide suitable blood transfusion samples to patients, the blood bag should be kept at a uniformly maintained temperature to prevent deterioration during transportation. Therefore, this paper presents a blood monitoring and management system for use in hospitals. This system may continuously report the temperature of the blood bank refrigerator, track the location of a blood bag to increase staff operation efficiency, and can confirm that the assigned blood bag was transported to the intended patient in need of transfusion. We developed and demonstrated the clinical usability of the combined blood temperature management and tracking system using a ubiquitous sensor network and RFID (Radio Frequency Identification) technology.

Keywords: RFID, Sensor network, Location tracking system, Blood.

1 Introduction

For the development of ubiquitous healthcare, the use of RFID (Radio Frequency Identification) technology and Sensor Network is becoming more commonplace but there is still little research on the simultaneous use of these two systems together as one application. These systems can be used to greatly improve the tracking of blood used in transfusions, as the blood must match the intended patient and should be

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 506 – 517, 2006.

tracked from the time it leaves the blood bank to the time it arrives for use in transfusions, in order to ensure that the blood was handled according to regulations [1, 2]. Blood should be kept at a fixed temperature. Blood that has deteriorated during transportation or while in storage must not be supplied to the patient. According to the Britain's National Blood Service report in 2000, 4.59% of the blood in stored blood banks of their hospitals was lost, and this percentage of lost blood may be greater in Korea's hospitals [3]. Therefore, there is a great need to construct a system using the Location Tracking Service and the sensor network that hospitals can use to measure blood temperature during both storage and transportation of blood bags, and to confirm that good-quality blood is supplied to the correct patients.

The blood bank currently operates the entire system manually, where the medical staff delivers blood to the location of transfusion after taking it out of refrigeration storage. The reasons why blood is not used for transfusions are because it was too old or there was an inadequate supply, or because the hospital administration denied use of the sample. Blood is always discarded if improper storage methods were used and by an increase in temperature resulted. Approximately thirty minutes after whole blood is removed from a 4℃ refrigerator and left to sit at room temperature, the red corpuscle becomes hemolytic; this decreases the lifetime of the blood because it causes excessive condensation and metabolism [1]. Thus, it is very important to keep blood at a temperature of 2~6℃ in order to maintain its quality and stability. Also, blood used for transfusions should be assigned to the correct patient. Accidents have been reported where the medical staff have inappropriately labeled the blood bags, mixed inappropriate blood samples together, or performed inaccurate adaptability tests [4].

We developed a 3T (Time, Temperature, Tracking)-enhanced system to prevent patient-blood mismatching and to obtain better temperature management of the blood samples by using a sensor network in blood banks and a RFID sensor tag that is placed directly on the blood bags. This system can track the movement of blood bags in designated time intervals (Time) and can monitor the change in blood temperature (Temperature) to provide more efficient, higher quality, and correct blood transfusions. The system can also generate data reports that medical personnel can share. Moreover, the need for an automatic system for transporting blood bags will help to reduce both the time and effort of medical staff. For these reasons, we used the Location Tracking System to track the location of blood bags and to prevent deterioration of blood that is being transported.

2 RFID and Sensor Network Using Zigbee

RFID is used to discriminate between objects that have a unique RF-tag, and this allows information to be processed specifically for each labeled object. RFID consists of a RF-tag, a RF-tag reader and operation software. The RF-tag reader can recognize the tag in 0.01~0.1 second and thus used in real-time application. The recognition rate is more than 99.9% in an area of 0~5 m, making it possible to communicate in a full-duplex mode, which saves a maximum of 64Kbyte of data [5]. The RFID can use

various ISM public frequency bands between 125 KHz and 2.45 GHz. Presently, the high frequency band RFID of 13.56 MHz is practically used in traffic cards in Korea because of the low tag cost compared to that of the low frequency band. The RFID is also divided into passive and active tags according to battery usage. The active RFID tag has a battery and can attach to various sensors.

The IEEE 802 standardization group defines the protocol standard according to various transmission rates and distances, such as the 802.11 WLAN and the 802.15.1 Bluetooth [6]. Among these standards, Zigbee, which is based on 802.15.4 for the MAC and PHY layer protocols, is frequently used in monitoring and controlling applications that are low power, low rate, and low cost for wireless networks. Zigbee uses the 2.45 GHz ISM band and accesses the channel by the CSMA-CA method. Zigbee is useful for sensor networks because it can extend to a wide area, being able to connect to 255 devices within a network, transmit data at a maximum of 250 Kbps, and support mesh network configurations [7].

3 Materials and Methods

3.1 Hardware

(1) Sensor, RFID tag & read/writer

We used the Crossbow Technology MTS420CA sensor to record the temperature of the refrigerator, the blood bank room temperature, and the temperature of the blood bag. The MTS420CA is used with the MICAz mote, which was developed by UC Berkeley to monitor the temperature, humidity, light acceleration, etc. The IEEE 802.15.4 is used to transmit the temperature data to the sink node, which is a MIB510CA which is also attached to the MICAz platform mote. Each sensor node is powered by two AA batteries and the signal from these sensors can reach 20~30 m distance but they can only operate for 10~15 hours in high power consumption mode, which does not have any programmed sleep intervals [8].

For the RFID temperature sensor, tag, and tag reader, we used the TempSens from KSW Co., which is an active RFID tag using an ISM band of 13.56 MHz. This has a built-in paper type battery that can last over 16 months and has enough SRAM memory to save 64 measurements of temperature data (Table 1) [9].

Table 1. Sensor, RFID tag and read/writer hardware specification

	Sensor & RF module	RFID tag & read/writer
Model	Crossbow Technology MTS420CA, MPR2400, MIB510CA	KSW TempSens, Inside
Frequency	2.4 GHz ISM band	13.56 MHz ISM band
Standard	IEEE 802.15.4	ISO 15693-3
Interface	RS-232C	USB
Data rate	250Kbps (57600 bps baud rate)	Upper 115200 bps baud rate
Operation Temperature	40 ~ 123.8℃	-15~+50℃ (tag), 20~70℃ (read/writer)
Etc	±0.5℃ at 25℃ accuracy	Data memory for 3 methods (all, threshold, max/min)

(2) Location Tracking System

The Location Tracking System is frequently used to send and receive small items using the container shown in Fig. 1. This system consists of a host computer, container, station, operator, controller, shift controller, and other components [10]. The host computer completely manages the entire system, and the station component sends for and receives the container. The operator loads the container and then sends the container to the final destination by having the container follow the tracks assigned by the controller and the shift controller.

In this paper, we used the Auto Track System from the SFA Co., which has been developed to be compatible with Siemens's equipment. The host computer met the following specifications of being a Pentium 4 CPU with 2.53 GHz, 512 MB of RAM, and 40 GB of HDD.

Fig. 1. Container, station and operator of the Auto Track System

(3) Others

We used the IBM ThinkPad R40 as the laptop computer for the blood bank which was attached to the sink node and the RFID reader. The HP TC1100 and the HP iPAQ RW6100 were used for the tablet PC and the PDA (Personal Digital Assistants), respectively. The DB Server was a Pentium 4 PC which was a CPU with 2.8 GHz, 200 GB of HDD, 1 GB of RAM, and was embodied with a MSSQL Server2000.

3.2 System Configuration and Data Gathering

The whole system configuration, the data acquisition process, and the configuration of the Location Tracking System from the blood bank to the place of transfusion are described in Fig. 2. The process begins with the refrigerator located inside the blood bank. In it is a sensor that configures the sensor network using Zigbee RF communication with the outside sink node. The data is then simultaneously sent to both the laptop computer and the RFID reader. Both the temperature and the blood bag information are stored in the DB Server, which is available through the WLAN within the hospital and is also connected to the HIS (Hospital Information System). This allows medical staff to access the information via the web server within the WLAN limits.

When the blood is taken from the blood bank refrigerator, the Location Tracking System transports the blood from the blood bank's station to the designated final destination. At this time, the host computer and controller determine the container's

track and alert the medical staff to the arrival of the containers. The host computer shows where the container is located at any given time, allowing medical staff to track the blood and decide whether or not to send it back depending on their readiness to receive it. Also, the host computer can be accessed by the DB Server, which allows users to query the blood location and the time the blood was released from the blood bank by using their monitoring devices.

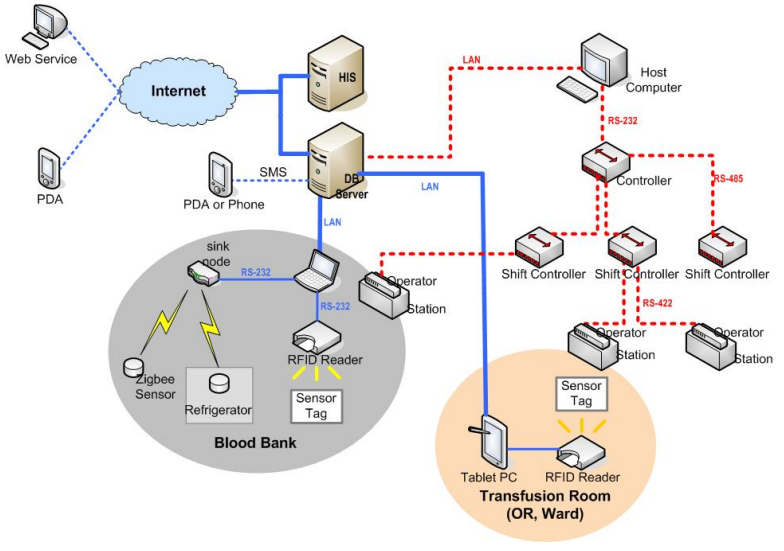


Fig. 2. Combined configuration of the temperature monitoring and the location tracking system

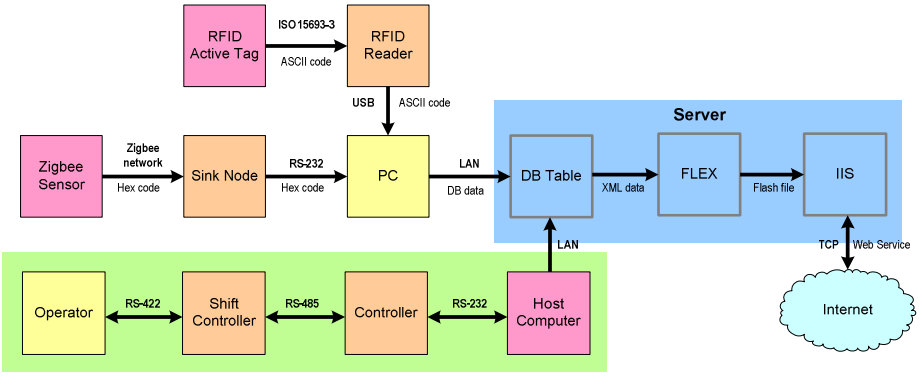


Fig. 3. Data gathering flow chart

A more concrete flow of data acquisition for the system described above is presented in Fig. 3. The cluster of the blood band is divided into two kinds of connections which are centered on the laptop PC. The laptop PC acquires the raw

data, as a hex code for the Zigbee sensor network and as an ASCII code for the RFID tag reading, from each of these connections. Thereafter, the server receives the data from the laptop to compose the DB table. At this time, the information on the location and time the blood was sent from the blood bank is saved in the DB. The DB Server converts this real-time information into XML script and the FLEX program then converts it into Flash form, enabling users in remote places to access the information via the web using Internet Explorer. The programs used in the sensor network, RFID reading, and the PDA application are realized with Microsoft Visual C++ 6.0, C#.NET, and .NET Compact Framework, respectively.

4 Results

4.1 Blood Transfusion Process

To verify the usability and efficiency of the system described above, we tested the system in the Shin-chon Severance Hospital located in Seoul, Korea. To prevent indirect deterioration of blood, the sensor network using the Zigbee mote and the temperature sensor installed in the blood bank refrigerator were used. This sensor measures the temperature inside the refrigerator and transmits measurements to the sink node and the laptop, which is connected to the DB server through WLAN within the hospital. If the temperature inside the refrigerator were to reach a temperature not suitable for blood storage, the DB server would send a SMS message to alert the administrator of the problem. When donated blood first arrives at the blood bank, the

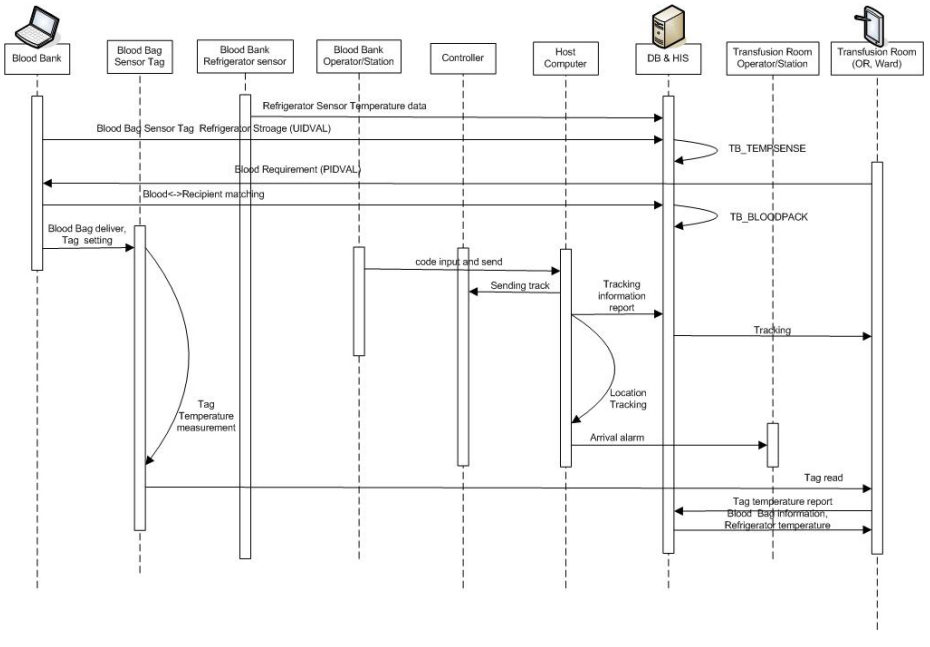


Fig. 4. Sequence diagram starting from the blood donation to the blood transfusion

medical staff instantly labels the blood bags with unique RFID tags and stores them in the refrigerator until needed. When blood is requested for a transfusion, the blood bank saves the blood bag information collected during storage and programs the tag to measure the temperature of the blood bag until it is received by the medical staff waiting to receive the sample. As the blood bag is transported to the final destination station via the Location Tracking System track, the host computer estimates the container's location at every station en route, and records this information in the DB server. Therefore, the remote administrator or the medical staff waiting at the final destination can know where the blood bag is at any given time. The host computer can also inform the destination station of the blood container's estimated time of arrival. Upon arrival, the destination station reports the temperature of the storage refrigerator prior to delivery and the temperatures of the blood bag during delivery, as measured by the RFID tag. The temperature of the blood is the most important environmental information to deciding whether the blood is suitable for use in a transfusion (Fig. 4).

We measured the temperature of the blood bank refrigerator in five-minute increments, because temperature does not fluctuate significantly within seconds in a controlled environment. Although the storage temperature is continuously monitored, the RFID tag on the blood bag not only contains this information but also the duration of storage time, and provides the blood bag with a unique ID. When blood is requested, the blood bank programs the RFID sensor to measure the temperature in pre-determined time intervals. A used RFID tag can only save 64 measurements of temperature data. Assuming it would take approximately an hour to transport the blood, we programmed the tag to measure the temperature in one-minute time intervals (Fig. 5).

As shown in Fig. 6, the blood is moved through the Location Tracking System. The host computer monitors all moving containers and provides their location, temperature, and the time the sample left the blood bank (Fig. 6 (d)).

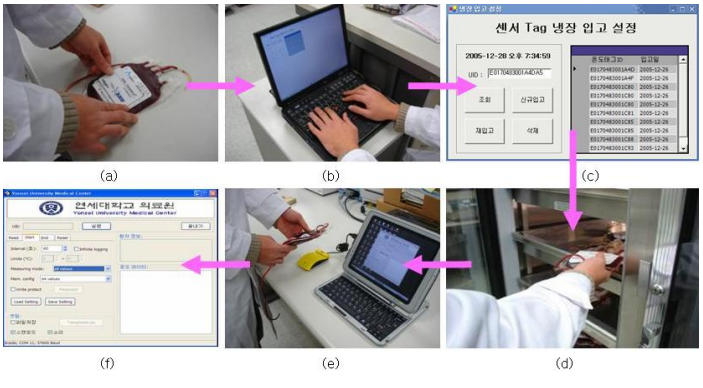


Fig. 5. Storage/take-out process of blood: (a) Attaching the RFID tag on the blood bag, (b) Storage set up, (c) Storage software, (d) Storage, (e) Tag setting after removal, and (f) Software used for tag setting

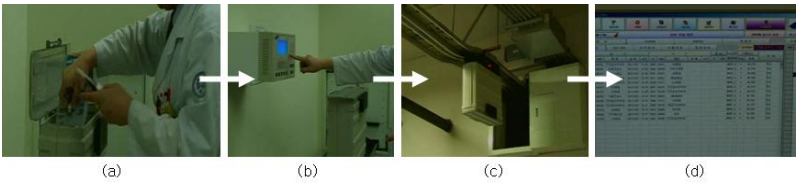


Fig. 6. Transport of blood using the Location Tracking System: (a) Input of the blood bag into the container, (b) Programming the destination, (c) Container moving along the track, and (d) Screenshot of the host computer tracking all containers

Fig. 7. Management system reporting the variation in temperature of the blood bag before a transfusion

Medical staffs always verify that the temperature of blood meets blood handling regulations, and that the intended patient and the delivered blood match, before the transfusion is performed (Fig. 7). When the RFID reader reads the tag, the temperature information during transport is first shown in the tablet PC. The storage temperature of the refrigerator in the blood bank also helps the medical staff determine whether the blood should be used for transfusion.

A remote administrator can use the DB data to query the blood temperature and patient information, to track deterioration of blood quality, or to confirm that a sample was used in a previous transfusion, as illustrated in Fig. 8. The information of both the blood bag and the refrigerator can be displayed in the same window as graphs, and a table can be generated to include the RFID tag ID, temperature and time at PDA.

To examine the possibility of using the Blood Management and the Location Tracking System as a real application, we tested the error range of the temperature sensor tag. The reader can recognize a RFID tag on the blood bag when held within 3 cm of the reader. If two or more tags are placed within this recognition range, the reader will not read any of the tags. Five sensor tags were used to compare the measured temperature to that of a digital thermometer (5℃). This resulted in an insignificant difference of 0.5~1℃.

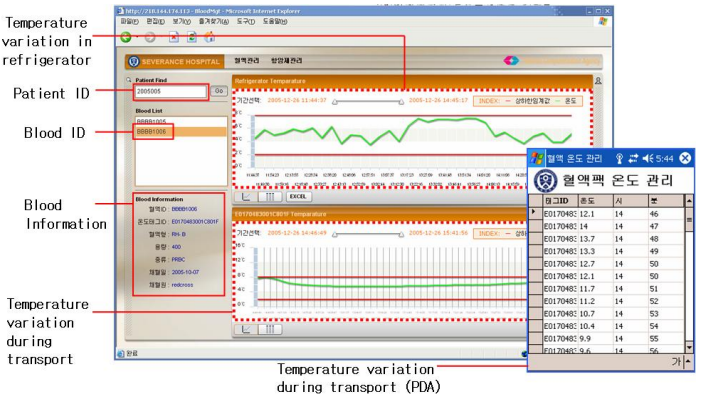


Fig. 8. Difference in temperature of a blood bag as displayed on Internet Explorer

Figure 9 represents the results of sensor 5's temperature rise an hour after the blood bag was removed from the refrigerator for transfusion. The reason this sensor tag consistently reported the highest temperature is because the blood bag with this sensor was placed on top of the other bags and therefore had the most contact with room temperature air. The graph indicates that this blood can no longer be used for transfusion because it exceeded 8℃ after 45 minutes, and suggests that the bag could have been used within 30 minutes after removal from the refrigerator because a temperature of 6℃ is still within regulations for blood transfusion.

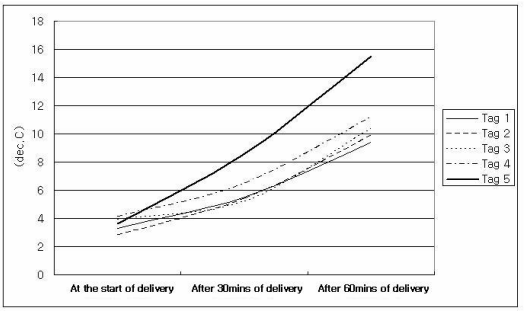


Fig. 9. Changes in temperature of the blood bags after removing them from the refrigerator

The time it takes to send a blood bag by the Location Tracking System can directly affect the rise in temperature as shown in Fig. 10. Most requests for blood were made during the normal working hours over the course of a 24-hour period. Deliveries took an average of 8~9 minutes. They took only 7~8 minutes except in cases where an operation was rescheduled and the previously arrived container was sent back. Moreover, excluding the 3.7% of containers sent back more than five times due to re-operation, the remaining containers do not take more than 15 minutes to be sent (Table 2). As Fig. 11 illustrates, often times the containers from the previous day are

sent to the storage station at the blood bank around 5:00 A.M. This increased the average time it took for a sample to reach its destination. Therefore, our system can be used as a reasonable way to automate the transportation of blood. This system will deliver blood in a timely manner, as long as medical staff realizes the possible back-log that could occur at 5:00 A.M.

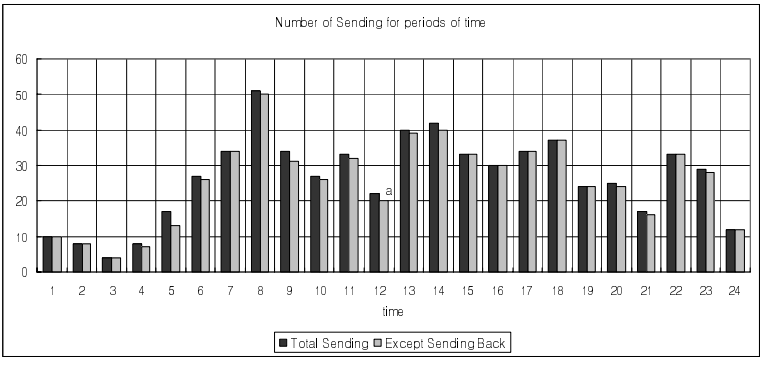


Fig. 10. Number of containers sent by the blood bank over a 24-hour time period

Table 2. Sending rate and average time of sending

Sending rate of blood bank among the all sending results in hospital (%)	16.04781
Average time of sending (min)	8.2884
Probability of re-operation (%)	5.07
Excessive probability of re-operation (%)	3.17
Average time of sending except excessive probability of re-operation (min)	7.6514

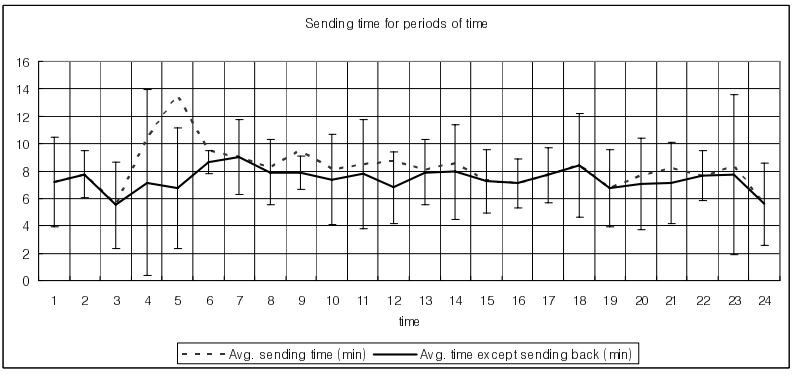


Fig. 11. Sending time and variance of containers sent from blood bank over a 24-hour period of time

5 Conclusions and Discussion

The hospital blood bank is in charge of managing blood bags from the time they are received from the blood donor to the time they are sent to the blood recipients for transfusion. Blood is very sensitive to temperature and should be stored in a temperature-stable environment, such as a refrigerator, to prevent deterioration during storage and transportation. Before the blood transfusion can take place, a number of tests are first performed by the medical staff to determine whether the blood is suitable for transfusion and to confirm the temperature of blood bag. However, the blood bank's storage facilities and equipment are still susceptible to power supply failures and human error, as they manually report the temperature every four hours [11]. Therefore in this paper, the blood bank sensor network system and the RFID tag for use during blood transport were developed to be more effective than manpower alone, while having the ability to share data and provide correct provisions of blood. The Location Tracking System proved useful, as we were able to track the location of moving blood bags and the time required of the medical staff was reduced, freeing them to do other necessary tasks.

Our test of the system proved that a more correct and analytical data history can be obtained than with the existing fragmentary management system, and we made it easy to monitor the real-time temperature variance of the blood samples. Based on this systematic blood management system, it is possible to decrease the rate of human error, the negative side effects of using poor quality blood for transfusions, and the rate of blood that is discarded. While our system makes managing blood bags simple and reliable, it also has a few technological shortcomings. The RFID tag which has a built-in sensor and battery is still too expensive to introduce to most medical centers, as it seems to be technically verified by a reliable organization. Also, the lifetime of the sensor battery is too short to be practical and must be co-developed to use with both the sensor network and the RFID. Finally, it is necessary to develop more graphical PDA programs to increment the mobility of the tag reader. It would be ideal if the container could be controlled thermostatically to preserve the temperature of blood bags throughout the transportation process.

Acknowledgement

This study was supported by a grant of the Korea Health 21 R and D Project, Ministry of Health and Welfare, Republic of Korea (02-PJ3-PG6-EV08-0001) implemented A Study on Experiments of Management of Blood Temperature with RFID Temp. Sensor & Management of Anticancer Medicine with Wireless Sensor Node, NCA (National Computerization Agency)'s USN Field Test. .

References

[1] Blood Center, the Republic of Korea National Red Cross. http://www.bloodinfo.net/
[2] Ministry of Health and Welfare. http://www.mohw.go.kr/index.jsp
[3] The National Blood Service (2000). http://www.blood.co.uk/

[4] Using RFID Technologies to Reduce Blood Transfusion Error, Joseph Dalton, PhD, White Paper by Intel Corporation, Cisco Systems, San RAaffaele Hospital (2005)
[5] Fundamentals and Applications in Contactless Smart Cards and Identification, G. Lee, YoungJin.com (2004)
[6] Zigbee Alliance Tutorial, Bob Heile, Zigbee Alliance (2005)
[7] Zigbee Network Layer Overview, Ian Marsden, Zigbee Alliance (2005)
[8] Crossbow Technology, Inc. http://www.xbow.com/
[9] KSW Microtec. http://www.ksw-microtec.de/www/startseite_de.php
[10] SFA Co., http://www.sfa.co.kr
[11] Blood Center, Laboratory Medicine, Severance Hospital. http://www.severance.or.kr/medical_guide/dept/lab/blood_center/

Energy Efficient Utilization of IEEE 802.11 Hot Spots in 3G Wireless Packet Data Networks

F. Ozan Akgül and M. Oğuz Sunay

Koç University,
Department of Electrical & Electronics Engineering,
Rumeli Feneri Yolu Sarıyer, Istanbul 34450, Turkey
fakgul@ku.edu.tr, osunay@ku.edu.tr
http://wireless.ku.edu.tr

Abstract. The third generation wireless networks and wireless local networks possess complementary characteristics. Recently, there has been significant interest in providing algorithms and specifications that enable their inter-operability. In this paper we propose a novel cross-network, cross-layer algorithm that jointly performs 3G resource allocation and ad-hoc mode WLAN routing towards effectively increasing the performance of the 3G system. The metrics used in this joint design ensures that multi-user diversity is exploited without causing user starvation in the 3G system and the WLAN assistance does not cause an unfair treatment to any of the mobiles from a battery usage point of view. Furthermore, the design attempts to select the WLAN route so that the assistance does not become a major part of the internal WLAN traffic.

1 Introduction

With the ever increasing use of the Internet there is a significant interest in making this technology available anywhere, anytime. To this end, the recent research in wireless systems has focused on providing high speed packet data access. Two complementary wireless technologies are gaining momentum to realize this goal: wireless local area networks (WLANs) providing high data rates over localized, small geographical areas (also referred to as hot spots), and third-generation (3G) cellular systems designed to provide lower data rates over wide geographical areas.

Given the clear demand for both, and their complementary characteristics, there has been significant interest in providing specifications for the inter-operability of 3G and WLAN systems. Both of the Third Generation Partnership Projects (3GPP and 3GPP2) have taken initiatives to develop cellular-WLAN interworking architectures that would be compatible to the existing 3G cellular system specifications of WCDMA and cdma2000 [1,2]. The goal is to provide cellular users seamless WLAN access where available and provide rates not achievable by 3G systems alone. Work on this front has focused on authentication, billing, seamless QoS and application-level services provisioning and roaming.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 518–529, 2006.

Both 3GPP and 3GPP2 provide specifications for the cellular-WLAN inter-operation when the WLAN system operates in the access network mode. However, the WLAN systems may be configured to operate in ad-hoc network mode as well. There has also been work in the literature that discuss the inter-operation of ad-hoc network mode WLAN with cellular systems [3-5]. In this case, the cellular system may be considered to be furnished with a relaying capability which would increase the overall coverage and capacity of the cellular system. This is because mobile terminals with channels experiencing low signal-to-noise ratios (SNRs) to the base station may observe better indirect, relayed links thereby increasing the observed data rate and/or reducing the power consumption. Clearly dual-network terminals would be necessary in this case as well.

In this paper we investigate the ad-hoc network mode WLAN and 3G wireless packet data integration where the cooperation would possibly enhance the cellular system capability. The 3G system under consideration is the North American IS-856 rev. 0 system (HDR) [6] which is a data-only cellular system providing peak rates of up to 2.4 Mbps over a 1.25 MHz bandwidth. Embedded in the area are hot spots (HSs) that are also covered with WLANs operating in the ad-hoc mode. The integration of the cellular and WLAN networks should enable the base station to know at any given time whether a dual-network mobile terminal is inside a given hot spot or not. Then, the cellular system will have the option of relaying information to the mobile terminal residing inside a hot spot via a number of other mobile terminals acting as relay nodes. For this scenario, we propose to jointly establish the cellular system resource allocation and the ad-hoc WLAN network routing schemes using a cross-network, cross-layer platform. While the IS-856 system will intend to increase the multi-user diversity gains through proper use of ad-hoc routing inside the hot spot, the routing algorithm will attempt to ensure that an energy fair route that utilizes as few of the WLAN resources as possible is set aside for this purpose.

The rest of the paper is organized as follows: next we give a brief overview of the 3G IS-856 rev. 0 wireless packet data system and its resource allocation procedure. We then discuss the most common ad-hoc routing protocols that take battery use into account. We propose a new cross-network, cross-layer joint cellular system resource allocation and WLAN ad-hoc system routing algorithm for the coordinated 3G-WLAN system. After briefly describing the simulation environment we present detailed simulation results for the proposed set-up and finally we present conclusions to the paper.

2 Overview of the IS-856 System

The wireless 3G system under consideration in this paper is the recently standardized 3G CDMA system for packet data, IS-856, otherwise known as HDR (High Data Rate) [6]. The HDR system divides the time into slots of length 1.67 ms and allocates all of its resources to a single user at a given time slot. Based on the observed channel quality between the base station and the served user at a given time, the modulation and coding levels are adjusted to provide

the maximum possible transmission data rate. The information data is encoded in blocks called physical layer packets. For some of the data rates, the physical layer packets span multiple time slots. The available data rates in the IS-856 rev. 0 system are given in Table 1 along with the associated packet size, modulation and coding levels and the number of time slots necessary to transmit the physical layer packets.

Table 1. Available data rates in IS-856

Data Rate (kbps)	Time Slots	Packet Size (bits)	Code Rate	Modulation
38.4, 76.8, 153.6, 307.2, 614.4	16, 8, 4, 2, 1	1024	1/5	QPSK
307.2, 614.4, 1228,8	4, 2, 1	2048	1/3	QPSK
921.6, 1843.2	2, 1	3072	1/3	8-PSK
1228.8, 2457.6	2, 1	4096	1/3	16-QAM

At the heart of the IS-856 system there is a scheduler that selects which user to service at a given time instance. The choice of the scheduling algorithm affects the overall system throughput as well as the average delay experienced by users in between successive accesses to the system. The throughput-optimal scheduling rule is one where the user with the best channel conditions is scheduled for service for each time slot. In such a scenario, the larger the number of users in the system, the more likely it is to find a user experiencing a really good channel resulting in a better system throughput. This is referred to as multi-user diversity in the literature. The optimal scheduling algorithm would be impractical as users closer to the base station would almost always observe better channel conditions and thus would grab the system resources continuously. Then, ideally scheduling algorithms that provide fairness across subscribers while utilizing multi-user diversity as much as possible are desirable. The study of scheduling algorithms is an active research topic. In this paper we will utilize the exponential rule [7] since this rule has been shown to have a very good fairness-throughput trade-off performance.

To describe the exponential rule properly, let us first define the following: t_s is the length of the time slot (=1.67 ms for the IS-856 system), $r_i(kt_s)$ is the data rate supported by user i at the k'th time slot, $\overline{r_i(kt_s)}$ is the average data rate observed by user i defined over a long sliding window of length T slots spanning the time $[(k-1-T)t_s,(k-1)t_s]$, $l_i(kt_s)$ is the number of slots user i has spent without service and $\overline{l(kt_s)}$ is the average of latencies observed by all users up until time slot k. Then, for the k'th time slot the exponential rule selects user j such that

$$j = \arg\max \frac{r_i(kt_s)}{\overline{r_i(kt_s)}} \exp\left(\frac{l_i(kt_s) - \overline{l(kt_s)}}{1+\sqrt{\overline{l(kt_s)}}}\right) \tag{1}$$

In (1), a large latency observed by one of the users relative to the overall average latency results in a very large exponent, overriding the channel conditions and leading to the large latency user getting priority. On the other hand, for small weighted latency differences, the exponential term is close to 1 and the policy is only ruled by the users' channel conditions relative to their own means.

3 Energy-Aware Multi-hop Routing in the WLAN Network

Lacking network infrastructure, wireless ad-hoc networks have no routers planning or overseeing the data transmission between two nodes. Instead, the nodes themselves function as routers and they discover and maintain routes to other nodes in the network. Several routing protocols have been proposed in the literature for ad-hoc networks. In general, these protocols can be divided into two broad classes: table-driven, or on-demand routing protocols.

Table-driven protocols require each node to maintain an accurate routing table in which information regarding every possible destination node is maintained at all times. The changes in the network topology is handled by sending update broadcast messages. Several table-driven protocols have appeared in the literature. These vary in the information stored at the routing table and how information updates are handled. The on-demand routing protocols, on the other hand, create routes only when requested by a source node. Upon demand, the source node initiates a route discovery process which lasts until a route is found or all possibilities are exhausted. Once a route between two nodes is established, this route is maintained by a route maintenance procedure until it is no longer desired or until the destination node becomes inaccessible by any means.

In wireless ad-hoc networks most nodes will operate on batteries. For this reason, minimization of the overall battery consumption and fair distribution of this consumption across the nodes become an important issue. By incorporating the current power levels into the routing tables in table-driven protocols and in the route discovery messages in the on-demand protocols, a route selection based on power consumption is possible. Such protocols should aim to select the path that minimizes the total power needed for the transmission between the source and destination nodes while minimizing the power consumption of all of the nodes. A number of power-efficient routing protocols have been studied in the literature for wireless ad-hoc networks that achieve one or both of these goals. The Maximum Total Transmission Power Routing Protocol (MTTPR), aims to find the route where the total transmission power used is a minimum [8]. MTTPR usually selects routes with more hops than other algorithms. This may not be desirable since a route with multiple routes will cause greater end-to-end delay. Perhaps the biggest disadvantage of the MTTPR protocol is that while it aims to select the route with the smallest overall transmission power, it pays no regards to the individual power levels of the nodes. The Minimum Battery Cost Routing (MBCR) aims to correct this by associating a cost function with every node that is inversely proportional with its remaining battery level

[9]. The protocol aims to select the route with the minimum total cost function. While the protocol incorporates fairness in the battery usage across the network, it does not prevent selecting a route that includes a node with a critically low power level. The Min-Max Battery Cost Routing Protocol (MMBCR) aims to minimize the maximum battery cost function within the route [9]. While this protocol ensures that no critical node appears in the final route, it does not minimize the overall power consumption. An alternative, the Conditional Min-Max Battery Cost Routing Protocol (MMBCR) aims to choose the route with the minimum overall power consumption among the routes that all have the maximum battery cost function below a certain threshold [10].

4 Proposed 3G-WLAN Integration

In this paper we propose the inter-operation of 3G and WLAN networks when both networks are available on the same geographical area. Our goal is to enhance the multi-user diversity impact observed in the IS-856 system by allowing multi-hop routing within the hot spot as an intermediate step on route to the destination mobile terminal. Then, the IS-856 base station, employing the exponential scheduler of (1) will need to check after each scheduling decision whether the scheduled mobile terminal is a dual-network, active WLAN subscriber as well. In a tightly-coupled integration scenario, the registration information of the two networks can easily be shared. In a loosely coupled integration scenario, the mobile terminals can transmit back to the base station occasional messages regarding whether they are also an active WLAN user or not. This information could be integrated into the regular channel state feedback messages the terminals transmit every 1.67 ms in the IS-856 system.

If the scheduled user is not an active WLAN user, the service to that user will be completed within the 3G network without any changes to the IS-856 operation. If, on the other hand, the mobile is also a WLAN subscriber, the base station will need to modify the scheduling decision to select a WLAN user that will potentially act as a gateway on route to the initially scheduled mobile. The scheduling of the gateway mobile should be such that the wireless channel it experiences from the 3G base station is better than the scheduled destination mobile terminal.

Then, user k is scheduled to act as the gateway mobile when

$$k = \arg\max_{i \in A} \; r_i(kt_s) \tag{2}$$

where maximization is done across all mobile terminals that are currently in the hot spot and that are dual network capable. This set of terminals is denoted as the set A.

Once the potential gateway terminal is determined, the 3G base station will need to compare the achievable data rates of this mobile with that of the destination mobile. If the destination mobile has a larger or equal data rate than the selected gateway mobile, then it can be serviced directly without the need for WLAN assistance. If, on the other hand, the gateway mobile has a larger data

rate than the destination mobile, WLAN assistance is helpful. In this case, the destination mobile can be serviced at the gateway mobile data rate (assuming that a route can always be found within the WLAN so that the bottleneck for the data rate is always the wireless channel from the base station to the gateway mobile).

If multiple terminals result in the same, maximum data rate, ties may possibly be broken in such a way that the node with the highest battery capacity is chosen. Naturally, for this purpose, the 3G network base station needs to know the current battery levels of all dual-network terminals that are active WLAN users. It is possible to incorporate this information into the channel-state feedback the terminals regularly transmit in the IS-856 network.

After the selection of the gateway terminal, a route between this terminal and the destination terminal needs to be discovered. The route discovery may be handled within the WLAN network without any input from the 3G network. In fact, the 3G network does not need to know the route details at all. In the 3G-WLAN cooperation scenario, a number of factors need be taken into account when deciding on the multi-hop route. First, the use of the WLAN system towards bettering the 3G system performance should result in as little impact on the internal WLAN traffic flow as possible. End-to-end delay between the gateway mobile and the destination user should also be accounted for by selecting a route that offers a relatively fast transmission speed. Second, the routing protocol has to ensure that as little power as possible is used for this purpose. Furthermore, it has to make sure that the power drainage should be shared more or less equally by all of the WLAN users so that some level of fairness can be maintained. None of the power-aware routing schemes described in the literature provide a solution for this problem since none consider battery consumption and transmission rate simultaneously. In this paper we propose an Power-Aware Exponential Ad-Hoc Routing Protocol (PEAR). PEAR selects the route r between the gateway terminal and the destination terminal such that

$$r = \arg\max_{i \in B} R_i(t) \exp\left(\frac{c_i(t) - \overline{c(t)}}{1 + \sqrt{\overline{c(t)}}}\right) \tag{3}$$

where $R_i(t)$ is the normalized average throughput and $c_i(t)$ is the sum percentile battery capacities of the nodes for route i at time t, respectively. $\overline{c(t)}$ is the average of the sum percentile battery capacities of all possible routes. The set B is the set of routes where the minimum battery capacity of a node is above a given threshold. The normalized throughput for route i with D_i nodes and data rates of $R_{(n_i,n_{i-1})}(t)$ between nodes n_i and n_{i-1} can be calculated as,

$$R_i(t) = \frac{1}{D_i - 1} \sum_{k=1}^{D_i - 1} \frac{R_{(n_i,n_{i+1})}(t)}{R_{\max}} \tag{4}$$

where $R_{\max}$ is the maximum possible transmission rate in the WLAN system (e.g. 11 Mbps for IEEE 802.11b). The sum percentile battery capacity for route

i with D_i nodes each with current percentile battery capacities $c_{(n_i)}(t)$ is calculated as,

$$c_i(t) = \sum_{k=1}^{D_i} c_{(n_i)}(t). \tag{5}$$

Similarly, the average of the sum percentile battery capacities of all possible N routes is calculated as,

$$\overline{c(t)} = \frac{1}{N} \sum_{i=1}^{N} c_i(t). \tag{6}$$

From (3), it is clear that for routes that have a large sum percentile battery, the exponential term dominates the data rate term and thus favoring routes with greater battery capacities. This leads to a fairer distribution of battery consumption across the WLAN user population. The data rate term in (3) is also an important parameter in the route selection since it directly relates to the link utilization of a particular route within the hot spot. Relaying the packets to the destination node on a route that has the highest average throughput means the minimal disruption of the internal WLAN communications. Thus, the proposed routing protocol, PEAR provides a compromise between choosing the link with the largest average data rate and the route with the largest total battery capacity. When the total battery capacity of a certain route is greater than the average total batter capacity of all of the routes by more than order $\sqrt{\overline{c(t)}}$, the exponential term overrides the average route throughput and this route is more likely to be selected. For routes with lower battery capacities than the average total battery capacity of all routes, the argument is dominated by the average throughput term. When a certain route has significantly lower battery capacity, this route will be less likely to be chosen even if its average bit rate is high.

5 System Performance Evaluation

To assess the performance of the WLAN assisted 3G IS-856 system described above, we have performed detailed simulations. The simulations are composed of three stages: System Level Simulations, Physical Layer Simulations and Joint Resource Allocation and Routing Simulations.

In the system level simulations we consider a 2-tier 19-cell environment for the 3G IS-856 system. Here, the first tier has 6 and the second tier has 12 cells centered around the cell of interest. Each cell is considered to have a radius of 1 km in the layout. We consider various hot spot configurations within the center cell. HSs that are 250m, 500m and 750m away from the 3G base station are considered. The HSs are assumed to have radii of 100m or 200m. We assume that the 3G users that are outside the hot spot have velocities of 3 km/h and 3G users that have WLAN access inside the HSs are assumed to have velocities of 0.5 km/h. The channel model in both cases includes path loss, Rayleigh fading and shadow fading. The ITU Pedestrian-A model describes the path loss model [11].

Similarly, Gudmundson's shadow fading model is used to describe the process as a log-normal random process [12]. The small-scale Rayleigh fading has been modeled using a filtered Gaussian noise. The sampling rate for the simulations is 600 Hz. The simulations have been performed for 18000 slots corresponding to 30 seconds of real time.

We have then performed comprehensive physical layer simulations to find the SNR (E_c/I_0) values corresponding to the target 1% packet error probabilities for each of the system data rates listed in Table 1. Agilent's ADS 2005A package has been used to simulate the IS-856 air interface components. The minimum required E_c/I_0 values to support each of the data rates is given in Table 3.

Table 2. Minimum Required E_c/I_0 Levels for 1% Packet Error Rate

Rate (kbps)	Slots	E_c/I_0 (dB)	Rate (kbps)	Slots	E_c/I_0 (dB)
38.4	16	-11.68	614.4	2	-0.88
76.8	8	-9.31	1228.8	1	3.55
153.6	4	-6.14	921.6	2	1.58
307.2	2	-2.96	1843.2	1	7.73
614.4	1	-0.77	1228.8	2	3.62
307.2	4	-3.94	2457.6	1	11.19

Finally, we have performed the joint resource allocation and routing simulations for a total number of $N_{3G} = 32$ 3G users such that

$$N_{3G} = N_{HS} + N'_{HS} \tag{7}$$

where N_{HS} is the number of 3G users that are also in the WLAN hot spot and N'_{HS} is the number of 3G users outside the WLAN coverage. In this scenario, we investigate the performance of the joint resource allocation and ad-hoc routing scheme for 2 to 16 active users in the hot spot, corresponding to a penetration of 6%-50%.

For each user, the current supported data rate along with the battery level is assumed to be fed back to the base station for scheduling and, if necessary, gateway terminal selection. The feedback messages from the terminals are assumed to arrive at the base station error-free, but with a round-trip delay of 3 time slots. The base station keeps a track of the average observed data rates for each active user where the averages are computed using a sliding window of 1000 slots.

Once the scheduling and gateway terminal selection is performed, the ad-hoc route is determined using (3). It is assumed that routing is performed locally within the WLAN at the initiation of the gateway terminal and the 3G network need not keep track of the details. In practice, the WLAN assistance will provide throughput gains at the expense of a certain delay due to route discovery, and multi-hop transmission within the network. Such additional delay is not considered in the scheduling process. In fact, the scheduling algorithm of (1) is

assumed to consider only the delay due to resource allocation procedure of the 3G system.

The route selection requires the knowledge of the battery levels of the nodes as well as the data rates between the nodes. We assume that the WLAN system under consideration is the IEEE 802.11b system for which the data rate-range relationship is such that [13] data rates of 11 MBps is achievable for open field ranges of 160m and smaller, 5.5 Mbps is achievable for ranges of 160m-270m, 2 Mbps is achievable for ranges of 270m-400m, and finally 1 Mbps is achievable for ranges of 400m-550m. No WLAN link is available between mobiles that are at least 550m apart.

The battery consumption inside the WLAN system is modeled such that each packet transmission or reception consumes one unit from battery. For instance the source and the destination nodes will consume 1 unit of battery whereas all intermediate nodes on the route will consume 2 units since they both receive and transmit the packets.

Based on the data rates and battery levels of each node, all possible routes are compared using the metric given in (3) and the route that provides the maximum value is selected. Figure 1 shows the WLAN assisted 3G performance results along with the performance of the 3G system without the WLAN assistance in the same cell geometry. It is observed that as the number of users in the hot spot increases, the assistance of the WLAN becomes more useful. This is to be expected, as the number of users inside the hot spot increase, it becomes more likely to find a WLAN gateway mobile experiencing a channel much better than that of the original scheduled user. In other words, as the number of users in the WLAN increase, the WLAN assistance enhances the multi-user diversity gain even when the scheduler tries to be fair across the 3G users.

It is also observed that as the WLAN hot spot location moves away from the cell radius, higher gains are observed through WLAN assistance. For WLAN HSs close to the cellular radius, most of the users within the hot spot will observe good channel conditions. The likelihood of finding a user that has better channel conditions than that of the originally scheduled user will be smaller in this case. Indeed, when one looks at the percentage of times WLAN assistance is beneficial, it becomes clear that it is less likely to gain from WLAN assistance if the hot spot is closer to the cell center. Alternatively, for HSs that are closer to the cell boundaries, larger variations across users in terms of achievable data rates are observed. In this case, WLAN assistance achieves gains most of the times.

In Figure 1 the 3G system throughput sometimes increases and sometimes decreases as the WLAN penetration increases for both the 3G only and WLAN assisted system scenarios. The dual nature is completely due to the geometry of the cell in question. Recall that the simulations are performed keeping the total number of users in the cell fixed at 32. As more users are forced into the hot spot, the geometry moves further away from a uniform distribution of these 32 mobiles in the cell. If the WLAN hot spot is closer to the cell center, clearly more and more users will observe better channel characteristics and thus the overall system improvement will increase with increased concentration in the WLAN hot spot.

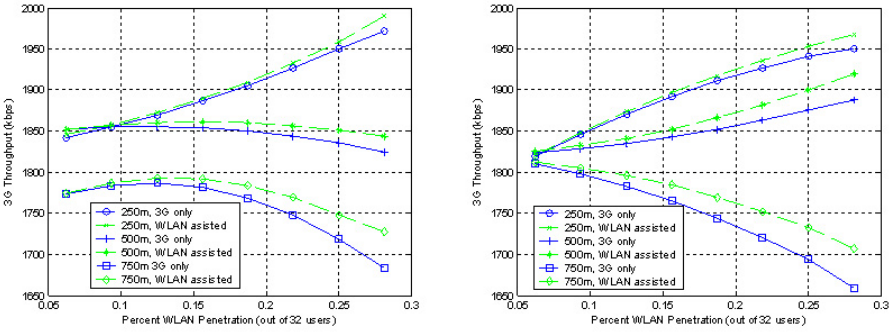


Fig. 1. Impact of the WLAN Assistance on the 3G system performance when the WLAN radius is 100m and 200m, respectively

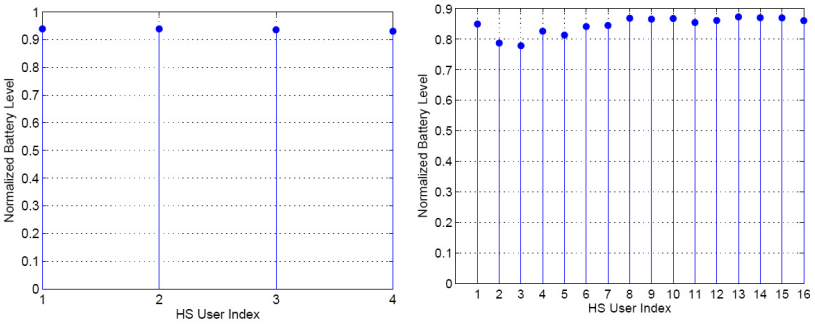


Fig. 2. Final Battery Levels of the Terminals (i. 4 of the 32 users are in the hot spot of radius 100m that is 500m away from the BS, ii. 16 of the 32 users are in the hot spot of radius 100m that is 500m away from the BS)

If on the other hand, the hot spot is closer to the cell boundary, increasing the WLAN user concentration will force more users to be located away from the cell center, decreasing the overall system throughput as the concentration increases.

Figure 2 shows the battery levels for selected number of users (4, 16 HS users, respectively) to demonstrate the fair selection behavior of our proposed scheme. The battery levels are the normalized values with respect to the full battery level. The graphs given here are for a WLAN hot spot that is 500m from the 3G base station and has 100m radius. Very similar graphs are obtained for hot spots that are 250 and 750 meters away from the 3G base station. Furthermore, the coverage area of the WLAN hot spot does not seem to affect the battery consumption fairness of the algorithm.

One important result we have obtained through the simulations is that the maximum number of hops in the selected route saturate at 3. This means that by

Table 3. Hop Percentages as a Function of HS User Concentration and HS Topology

100m Radius Hot Spot								
250m away from BS			500m away from BS			750m away from BS		
No Users	Hops	%	No Users	Hops	%	No Users	Hops	%
4	3G only	89.172	4	3G only	89.217	4	3G only	86.828
	0	2.6389		0	2.9889		0	3.4389
	1	7.4722		1	8.2444		1	9.5333
	2	0.7167		2	0.4444		2	0.1333
	3	0		3	0.1056		3	0.0667
16	3G only	59.322	16	3G only	59.278	16	3G only	56.267
	0	2.5833		0	2.5444		0	2.6944
	1	35.972		1	36.306		1	38.539
	2	2.1222		2	1.8722		2	2.5
	3	0		3	0		3	0
200m Radius Hot Spot								
250m away from BS			500m away from BS			750m away from BS		
No Users	Hops	%	No Users	Hops	%	No Users	Hops	%
4	3G only	89.956	4	3G only	89.05	4	3G only	87.683
	0	2.6333		0	2.7333		0	2.9389
	1	4.0167		1	3.7		1	4.4333
	2	2.8667		2	2.7944		2	2.6944
	3	1.5278		3	1.7222		3	2.25
16	3G only	58.967	16	3G only	58.711	16	3G only	56.656
	0	2.3444		0	2.6389		0	2.5278
	1	16.522		1	16.561		1	16.1
	2	13.2		2	13.639		2	15.328
	3	8.9667		3	8.45		3	9.3889

utilizing at most 2 intermediate nodes, the 3G packet is relayed to the destination. Table 3 provides the detailed results of percentages that a certain number of hops occur for the topologies as well as user concentrations considered.

One immediate result obtained is the percent increase in the occurrence of higher number of hops as the number of users in the hot spot increases. This result is expected since as the number of users increase so do the number of possible routes requiring more nodes. However, despite this tendency, the results clearly indicate that the proposed algorithm favors fewer hops. It is also observed once again that WLAN assistance is more useful as the number of WLAN users increase. Another observation is that as the coverage area of the WLAN increases so do the expected number of hops. The reason for this is that, with increased WLAN coverage, it is more likely that the distance between the gateway terminal and the destination terminal is far, requiring multiple nodes for relaying along the way. As the number of users further increase in this case, the expected number of hops further increase. This is because, given equal distribution of battery levels, the algorithm will favor links with larger average data rates, which would most likely result in multiple hops where each node is separated by a shorter distance.

6 Conclusions

In this paper we have investigated a possible system integration between the 3G IS-856 packet data system and the IEEE 802.11 WLAN operating in the ad-hoc network mode. We have proposed a cross-network, cross-layer approach to jointly determine how the 3G system resources are scheduled across the users so that a compromise is maintained between high network throughput and fairness across the user observed latency. The proposed scheme exploits multi-user diversity in the 3G system and employs a novel power-aware routing protocol, PEAR, that aims to find a compromise between selecting a route with high data rate and a route with large available battery capacity. Simulation results show improvements in the throughput performance of the 3G system when WLAN assistance is utilized. The proposed routing algorithm provides a fair use of battery capacity across the WLAN membership.

References

1. 3GPP, "Group Services and System Aspects: 3GPP Systems to Wireless Local Area Network (WLAN) Interworking - System Description (Release 6)," TS23.234. v.2.5.0, March 2004.
2. 3GPP2, "3GPP2-WLAN Interworking, Stage 1 Requirements," SP0087-0 v.0.5, 14 July 2003.
3. V. Sreng, H. Yanikomeroglu and D.D. Falconer, "Relayer Selection Strategies in Cellular Networks with Per-to-Peer Relaying," *Proceedings of the IEEE VTC-Fall 2003 Conference*, 2003.
4. H. Wu et.al., "Integrated Cellular and Ad-Hoc Relaying Systems: iCAR," *IEEE Journal on Selected Areas in Communications*, vol. 19, pp. 2105-2115, 2001.
5. H.Y. Wei, R.D. Gitlin, "Two-Hop-Relay Architecture for Next-Generation WWAN/WLAN Integration," *IEEE Wireless Communications Magazine*, vol. 11, no.2, pp. 24-30, February 2004.
6. TIA/EIA/IS-856, "cdma2000 High Rate Packet Data Air Interface Specification," 3GPP2, C.S0024, v4.0, Oct. 2002.
7. S. Shakkottai, A. Stolyar, "Scheduling Algorithms for a Mixture of Real-Time and Non-Real-Time Data in HDR", Bell Laboratories Technical Report, 2000.
8. S. Singh, C.S. Raghavendra, "PAMAS - Power Aware Multi-Access Protocol with Signaling for Ad-Hoc Networks", *ACM Computer Communication Review,* vol.28, no.3, pp 5-26, July 1998.
9. S. Singh, M. Woo, and C.S. Raghavendra "Power Aware Routing in Mobile Ad-Hoc Networks", *Mobile Computing and Networking*, pp. 181-190, 1998.
10. C-K. Toh, "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad-Hoc Networks," *IEEE Communications Magazine,* no.6, pp. 138-147, June 2001.
11. International Telecommunication Union, "Guidelines for Evaluation of Radio Transmission Technologies for IMT-2000," *Recommendation, ITU-R, M.1225*, 1997.
12. M. Gudmundson, "Correlation Model for Shadow Fading in Mobile Radio Systems," *Electronics Letters,* vol. 27, pp. 2145-2146, Nov. 1991.
13. Agere Systems, "WaveLAN 802.11b Chip Set for Standard Form Factors", *Preliminary Product Brief,* December 2002.

Author Index