

Mieso K. Denko Chi-Sheng Shih
Kuan-Ching Li Shiao-Li Tsao
Qing-An Zeng Soo-Hyun Park
Young-Bae Ko Shih-Hao Hung
Jong Hyuk Park (Eds.)

LNCS 4809

Emerging Directions in Embedded and Ubiquitous Computing

EUC 2007 Workshops: TRUST, WSOC
NCUS, UUWSN, USN, ESO, and SECUBIQ
Taipei, Taiwan, December 2007, Proceedings



ifip

 Springer

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Mieso K. Denko Chi-Sheng Shih
Kuan-Ching Li Shiao-Li Tsao
Qing-An Zeng Soo-Hyun Park
Young-Bae Ko Shih-Hao Hung
Jong Hyuk Park (Eds.)

Emerging Direction in Embedded and Ubiquitous Computing

EUC 2007 Workshops: TRUST, WSOC
NCUS, UUWSN, USN, ESO, and SECUBIQ
Taipei, Taiwan, December 17-20, 2007
Proceedings

Volume Editors

Mieso K. Denko

University of Guelph, Ontario, N1G 2W1, Canada, E-mail: denko@cis.uoguelph.ca

Chi-Sheng Shih

National Taiwan University, Taipei, 106, Taiwan, E-mail: cshih@csie.ntu.edu.tw

Kuan-Ching Li

Providence University, Shalu, Taichung, Taiwan, E-mail: kuancli@pu.edu.tw

Shiao-Li Tsao

National Chiao Tung University, Taiwan, E-mail: sltsao@cs.nctu.edu.tw

Qing-An Zeng

University of Cincinnati, USA E-mail: qzeng@eccc.uc.edu

Soo-Hyun Park

Kookmin University, Seoul, Korea, E-mail: shpark21@kookmin.ac.kr

Young-Bae Ko

Ajou University, Suwon, Korea, E-mail: youngko@ajou.ac.kr

Shih-Hao Hung

National Taiwan University, Taipei, Taiwan, E-mail: hungsh@csie.ntu.edu.tw

Jong Hyuk Park

Kyungnam University, Kyungnam, Korea, E-mail: parkjonghyuk@gmail.com

Library of Congress Control Number: 2007940866

CR Subject Classification (1998): C.2, C.3, D.4, D.2, H.4, K.6.5, H.5.3, K.4

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

ISSN 0302-9743

ISBN-10 3-540-77089-5 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-77089-3 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© IFIP International Federation for Information Processing 2007

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12199198 06/3180 5 4 3 2 1 0

Preface

This proceedings volume contains the papers presented at the workshops held in conjunction with the 2007 IFIP International Conference on Embedded and Ubiquitous Computing (EUC 2007), in Taipei, Taiwan, December 17–20, 2007. The main aim of these workshops is to bring together academics, industry researchers and practitioners to discuss and exchange state-of-the-art research results and experience, case studies and on-going research activities in the areas of embedded and ubiquitous computing, networking and communications.

The seven workshops held in conjunction with EUC 2007 were:

1. The Second International Workshop on Trustworthiness, Reliability and services in Ubiquitous and Sensor neTworks (TRUST 2007)
2. The Third International Symposium on Security in Ubiquitous Computing (SecUbiq 2007)
3. The Second International Workshop on Embedded Software Optimization (ESO 2007)
4. The Third International Workshop on RFID and Ubiquitous Sensor Networks (USN 2007)
5. The Third International Symposium on Network-Centric Ubiquitous Systems (NCUS 2007)
6. The First International Workshop on System and Software for Wireless SoC (WSoC 2007)
7. The First International Workshop on Ubiquitous UnderWater acoustic-Sensor Network 2007 (UUWSN 2007)

Each of these workshops addressed a particular topic related to the main theme of the conference and attracted a number of quality papers that complemented the main conference. The workshop organizers formed strong Technical Program Committees that helped in selecting high-quality papers for presentation and publication in the workshop proceedings.

Several individuals contributed to the success of these workshops. In particular, we would like to thank the EUC 2007 General Chair Edwin Sha and Program Chair, Tei-Wei Kuo for their guidance and support, and EUC 2007 Steering Co-chairs, Laurence T. Yang, Minyi Guo and Jane Liu, for their guidance as well as for giving us this opportunity. Last but not least, we would also like to thank the workshop organizers for their hard work which greatly contributed to the success of this event.

December 2007

Mieso K. Denko
Chi-Sheng (Daniel) Shih

The Second International Workshop on Trustworthiness, Reliability and Services in Ubiquitous and Sensor neTworks (TRUST 2007)

Workshop Organizers

Jong Hyuk Park, Laurence T. Yang, Sandeep Gupta, Ilsun You, Kuan-Ching Li,
David Chadwick, Eun-Sun Jung

Workshop Description

With the proliferation of wireless technologies, there is a fast-growing interest in ubiquitous environments (UE). UE enables one to create a human-oriented computing environment where computer chips are embedded in everyday objects and interact with the physical world. With a great potential to revolutionize our lives, UE also poses new research challenges. TRUST 2007 focused on the challenges and solutions for UE with an emphasis on trust-worthiness, reliability, and services.

In order to guarantee high-quality proceedings, we put extensive effort in reviewing the scientific papers. We received 51 papers from Japan, China, Korea, Hong Kong, Taiwan, Canada, UK, France, Italy, Norway, and USA, representing more than 50 universities or institutions. All submissions were peer reviewed by three Program Committee members. It was hard to select the presentations.

The workshop program contained 15 regular papers, which represents an acceptance rate of 29%. We congratulate the authors of accepted papers, and regret many quality submissions could not be included, due to the time limit of this program.

Our special thanks go to the Program Committee, who had the difficult task of reviewing the large number of papers in a relatively short time. Finally, we are also indebted to the members of the Organizing Committee.

TRUST 2007 Organization

Steering Co-chairs

David Chadwick
Eun-Sun Jung

University of Kent, UK
Samsung Advanced Institute of Technology, Korea

General Co-chairs

| | |
|------------------|---------------------------------------|
| Jong Hyuk Park | Kyungnam University, Korea |
| Laurence T. Yang | St. Francis Xavier University, Canada |
| Sandeep Gupta | Arizona State University, USA |

Program Co-chairs

| | |
|---------------|--------------------------------|
| Il-sun You | Korean Bible University, Korea |
| Kuan-Ching Li | Providence University, Taiwan |

Program Vice Co-chairs

| | |
|--------------------|--|
| Ching-Hsien Hsu | Chung Hua University, Taiwan |
| Eung Nam Ko | Baekseok University, Korea |
| Schahram Dustdar | Vienna University of Technology, Austria |
| Stefanos Gritzalis | University of the Aegean, Greece |

Publicity Co-chairs

| | |
|-----------------|--|
| Makoto Takizawa | Tokyo Denki University, Japan |
| Matt Mutka | Michigan State University, USA |
| Sheng-De Wang | National Taiwan University, Taiwan |
| Yunhao Liu | Hong Kong University of Science and Technology, Hong Kong |

Web Management Chair

| | |
|----------------|--------------------------|
| Byoung-Soo Koh | DigiCAPS Co., Ltd, Korea |
|----------------|--------------------------|

Program Committee

| | |
|------------------------|---|
| Agustinus Borgy Waluyo | Institute for Infocomm Research, Singapore |
| Andrew Kusiak | The University of Iowa, USA |
| Anind K. Dey | Carnegie Mellon University, USA |
| Antonio Coronato | ICAR-CNR, Italy |
| Byoung-Soo Koh | DigiCAPS Co., Ltd, Korea |
| Chaoguang Men | Harbin Engineering University, China |
| Chao-Tung Yang | Tunghai University, Taiwan |
| Chih-Yung Chang | Tamkang University, Taiwan |
| Cho-Li Wang | The University of Hong Kong, Hong Kong |
| David Simplot-Ryl | University of Sciences and Technologies of Lille, France |
| Deok-Gyu Lee | ETRI, Korea |

| | |
|-------------------------------|--|
| Emmanuelle Anceaume | IRISA, France |
| Evi Syukur | Monash University, Australia |
| George A. Gravvanis | Democritus University of Thrace, Greece |
| Giuseppe De Pietro | ICAR-CNR, Italy |
| Guihai Chen | Nanjing University, P.R. China |
| Hongbo Zhou | Slippery Rock University, USA |
| HHung-Yu Wei | National Taiwan University, Taiwan |
| Jason Hung | Northern Taiwan Institute of Science and Technology, Taiwan |
| JeongHyun Yi | Samsung Advanced Institute of Technology, Korea |
| Jianhua Ma | Hosei University, Japan |
| Jin Wook Lee | Samsung Advanced Institute of Technology, Korea |
| Karl M. Goeschka | Vienna University of Technology, Austria |
| Laborde Romain | University of Toulouse III, France |
| Marco Aiello | University of Trento, Italy |
| Mario Ciampi | ICAR-CNR, Italy |
| Massimo Poncino | Politecnico di Torino, Italy |
| Naixue Xiong | JAIST, Japan |
| Nicolas Sklavos | Technological Educational Institute of Mesolonghi, Greece |
| Nikolay Moldovyan | SPECTR, Russia |
| Ning Zhang | University of Manchester, UK |
| Oh-Heum Kwon | Pukyung University, Korea |
| Paris Kitsos | Hellenic Open University, Greece |
| Hwa Jin Park | Sookmyung Women's University, Korea |
| Qi Shi | Liverpool John Moores University, UK |
| Rodrigo Fernandes de Mello | University of Sao Paulo, Brazil |
| Slo-Li Chu | Chung Yuan Christian University, Taiwan |
| Taejoon Park | Samsung Advanced Institute of Technology, Korea |
| Vesna Hassler | European Patent Office, Austria |
| Weisong Shi | Wayne State University, USA |
| Xue Liu | University of Illinois at Urbana-Champaign, USA |
| Yan Solihin | North Carolina State University, USA |
| Yeong-Deok Kim | Woosong University, Korea |
| Yuan Xie | Pennsylvania State University, USA |

The First International Workshop on System and Software for Wireless SoC (WSOC 2007)

Workshop Organizers

Shiao-Li Tsao and ChingYao Huang

Workshop Description

Advances in system-on-chip (SoC) technologies make it possible to develop low-cost and compact-size ICs for information technology (IT) and consumer electronic products. Wireless or radio SoCs which provide wireless accesses are regarded as one of the most important categories. Successful stories such as Bluetooth, WLAN, and GSM SoCs encourage the development of SoCs for advanced wireless access technologies, and thus the research and development of advanced Wireless SoCs have attracted considerable interest from both academia and industry in recent years. Unfortunately, these advanced wireless systems, such as WiMAX and 4G, support rich applications and broadband accesses which make the SoCs very difficult to design and implement. Major issues such as the requirement development, system level model, system level design (SLD), and verification and validation for such complicated wireless SoCs need more investigations and studies. The hardware and software partitions and hardware and software co-designs of wireless SoCs are also important research topics. Embedded software is especially critical for wireless SoCs, since the system software and application software are both complicated. Code efficiency, low-power and small foot-print software are required for wireless SoCs which are usually employed in battery-operated and portable devices.

The goal of WSOC 2007 was to provide a forum for scientists, engineers, and researchers to discuss and exchange their new ideas, novel results, work in progress and experience on all aspects of system level design, HW/SW co-design, embedded software, research platforms and case studies for advanced wireless SoCs.

We selected 12 high-quality papers to be included in the WSOC 2007 program. We congratulate the authors of accepted papers. We also had two invited talks from industrial executives, who shared their experiences in designing wireless SoCs with us.

We would like to thank all the authors for their contributions to the program, the Program Committee members and external reviewers for reviewing and providing valuable comments to the submissions. We are grateful to Ken Loa from the Institute for Information Industry of Taiwan and Y.M. Yeh from Mobile Devices Inc. for their time and contributions to the invited talks. Finally, we would like to thank Chi-Sheng Shih and Mieso Denko, the EUC 2007 Workshop Co-chairs, for the guidance in the organization of the workshop.

Workshop General Co-chairs

Shiao-Li Tsao National Chiao Tung University, Taiwan
ChingYao Huang National Chiao Tung University, Taiwan

Program Committee

Hojung Cha Yonsei University, Korea
Chip Hong Chang Nanyang Technological University, Singapore
Chien Chen National Chiao Tung University, Taiwan
Sau-Gee Chen National Chiao Tung University, Taiwan
Fang Chen Cheng Alcatel-lucent Technology, USA
Sheng-Tzong Cheng National Cheng Kung University, Taiwan
Chuan Heng Foh Nanyang Technological University, Singapore
Carrson Fung National Chiao Tung University, Taiwan
Teck Hu Nokia Siemens Networks, USA
Joe Huang Alcatel-lucent Technology, USA
Wen-Yi Kuo Bandich, Taiwan
David Lin National Chiao Tung University, Taiwan
Shen Chieh Liu Mobile Devices Inc., Taiwan
Shiann-Tsong Sheu National Central University, Taiwan
Hsuan-Jung Su National Taiwan University, Taiwan
Ilenia Tinnirello University of Palermo, Italy
Jane Wang University of British Columbia, Canada
Hung-Yu Wei National Taiwan University, Taiwan
Wen Rong Wu National Chiao Tung University, Taiwan

The Third IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2007)

Symposium Organizers

Laurence T. Yang, Kuan-Ching Li, Ce-Kuen Hsieh, Qing-An Zeng, Weijia Jia, Yun Liu, Hao-Hua Chu

Symposium Description

Historically, ubiquitous systems have been highly engineered for a particular task, with no spontaneous interactions among devices. Recent advances in wireless communication and sensor and actuator technologies have given rise to a new genre of ubiquitous systems. This new genre is characterized as self-organizing, critically resource constrained, and network centric. The fundamental change is communication: numerous small devices operating collectively, rather than as standalone devices, form a dynamic ambient network that connects each device to more powerful networks and processing resources.

NCUS 2007 was the successor of the First IFIP International Symposium on Network Centric Ubiquitous Systems (NCUS 2005) held in Nagasaki, Japan and the Second IFIP International Symposium on Network Centric Ubiquitous Systems (NCUS 2006) held in Seoul, Korea. It offered a premier international forum for researchers and practitioners from both industry and academia to discuss hot topics and emerging areas, to share recent progress and latest results, and to promote cutting edge research and future cooperation on ubiquitous systems and ubiquitous networking.

We were very proud to receive 45 high-quality submissions. We conducted a rigorous peer-review process for each submission, with the great support of all Program Committee members as well as a group of external reviewers. Each paper was reviewed by three reviewers for content, accuracy and relevance to the scope of the symposium. We selected the 13 best papers out of 45 submissions in this program, representing an acceptance rate of 28.8%. These papers were classified into four major sessions.

The symposium Chairs would like to thank all the authors for their contributions and support of this symposium. We are very grateful to all the Program Committee members and other colleagues who helped us in the review process for this workshop. We are especially thankful to Chi-Sheng Shih and Mieso Denko for their support and guidance throughout the organizing process of the symposium.

Organizing Committee

Steering Chair

Laurence T. Yang, St. Francis Xavier University, Canada

General Co-chairs

Kuan-Ching Li, Providence University, Taiwan

Ce-Kuen Shieh, National Cheng Kung University, Taiwan

Program Co-chairs

Qing-An Zeng, University of Cincinnati, USA

Wei-jia Jia, City University of Hong Kong, China

Yun Liu, Beijing Jiaotong University, China

Publicity Chair

Hao-Hua Chu, National Taiwan University, Taiwan

Program Committee

Nael Abu-Ghazaleh, SUNY Binghamton, USA

Hesham H. Ali, University of Nebraska at Omaha, USA

Irfan Awan, University of Bradford, UK

Doo-Hwan Bae, Korea Advanced Institute of Science and Technology, Korea

Jacir L. Bordim, University of Brasilia, Brazil

Phillip Bradford, University of Alabama, USA

Jiannong Cao, Hong Kong Polytechnic University, China

Chichyang Chen, Feng Chia University, Taiwan

Xiuzhen Cheng, George Washington University, USA

Song Ci, University of Massachusetts Boston, USA

Jitender S. Deogun, University of Nebraska at Lincoln, USA

Dan Feng, Huazhong University of Science and Technology, China

Satoshi Fujita, Hiroshima University, Japan

Paulo Roberto de Lira Gondim, Universidad de Brasilia, Brazil

Dan Grigoras, University College Cork, Ireland

Hung-Chang Hsiao, National Cheng Kung University, Taiwan

Hai Jin, Huazhong University of Science and Technology, China

Ajay Kshemkalyani, University of Illinois at Chicago, USA

Hyunyoung Lee, University of Denver, USA

Liang-Teh Lee, Tatung University, Taiwan

Victor C.M. Leung, The University of British Columbia, Canada

Jiang (Leo) Li, Howard University, USA
Xiaolong Li, Morehead State University, USA
Kathy Liszka, University of Akron, USA
Wei Liu, Huazhong University of Science and Technology, China
Mario Donato Marino, University of Sao Paulo, Brazil
Koji Nakano, Hiroshima University, Japan
Nidal Nasser, University of Guelph, Canada
Mohamed Ould-Khaoua, University of Glasgow, UK
Jun Pang, University of Oldenburg, Germany
Marcin Paprzycki, SWPS, Poland
Dana Petcu, Institute e-Austria Timisoara, Romania
Wei Qin, Boston University, USA
Ilkyeun Ra, University of Colorado at Denver, USA
Won-Woo Ro, California State University-Northridge, USA
Huai-Rong Shao, Samsung, USA
Hong Shen, Computer Science, University of Adelaide, Australia
Randy Smith, University of Alabama, USA
Siang-Wun Song, University of Sao Paulo, Brazil
Rafael Timoteo de Sousa, Universidad de Brasilia, Brazil
You-Chiun Wang, National Chiao Tung University, Taiwan
Bin Wang, Wright State University, USA
Cho-Li Wang, The University of Hong Kong, China
Guojun Wang, Central South University, China
Guoliang Xue, Arizona State University, USA
Chu-Sing Yang, National Cheng-Kung University, Taiwan
Eiko Yoneki, University of Cambridge, UK
Liqiang Zhang, Indiana University at South Bend, USA
Jingyuan Zhang, University of Alabama, USA

The First International Workshop on Ubiquitous UnderWater acoustic-Sensor Network 2007(UUWSN 2007)

Workshop Organizers

Soo-Hyun Park, Chang-Hwa Kim, Young-Sik Jeong, Dongwon Jeong, Laurence T. Yang

Workshop Description

Underwater acoustic sensor networks (UW-ASN) have many potential application areas such as ocean monitoring and disaster prevention. Although more than two-thirds of the earth's surface is covered with water, including oceans, rivers and lakes, the oceans remain one of the last frontiers and are a treasure trove of resources. Oceans serve as the main arteries of transportation between continents, food supplies and natural resources retrieval such as oil and natural gas. Recently, researchers UW-ASN have been trying to apply sensor network concepts to underwater environments to be used in the field such as in resource inquiry, pollution supervision and catastrophe prevention.

UW-ASN is a new area of ubiquitous sensor networks in underwater environments which has challenges to be overcome such as in the long propagation delay resulting from the low speed of sound propagation, severely limited range-dependent bandwidth, attenuation and time-varying multipath propagation. All of the above distinct features of UW-ASN give birth to new challenges in the network protocol suite.

This workshop provides an opportunity for industry and academic professionals to discuss the latest issues and progress in the area of UW-ASN. The workshop publishes high-quality papers closely related to the various theories and practical applications in UW-ASN. Furthermore, this workshop gives researchers a chance to share creative ideas regarding UW-ASN with each other and with engineers from institutions around the world.

UUWSN 2007 was the first workshop on underwater sensor networks to be held in Asia. We had more than 33 papers submitted to this workshop and each paper was carefully reviewed by the internationally organized UUWSN 2007 Technical Program Committee (TPC) – three reviewers for each paper. We selected only ten excellent papers among them, representing an acceptance rate of 30%. We congratulate the authors of accepted papers and regret that many high-quality submissions could not be included, due to the limit in session time.

We had one keynote speech concerning ocean experiments in underwater acoustic networking adding to the content of our high-quality program.

On behalf of the board of the UUWSN 2007 workshop, we appreciate all the submissions to the program. We are grateful that Joseph A. Rice (Naval

Postgraduate School, US) accepted our invitation for the keynote presentation. We would also like to thank the TPC members and external reviewers for their efforts in reviewing the submissions. Finally, we would like to thank Chi-Sheng(Daniel) Shih (National Taiwan University, Taiwan) and Mieso Denko (University of Guelph, Canada), the workshop Co-chair, for the guidance in the organization of this workshop.

This workshop was partly supported by Kangnung National University ITRC (Research Center for Ocean Sensor Network System Technology) and the MIC (Ministry of Information and Communication), Korea, under the 2007 ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

Steering Co-chairs

Laurence T. Yang, St. Francis Xavier University, Canada
Soo-Hyun Park, Kookmin University, Korea

General Chair

Soo-Hyun Park, Kookmin University, Korea

Program Co-chairs

Chang-Hwa Kim, Kangnung National University, Korea
Young-Sik Jeong, Wonkwang University, Korea

Publication Chair

Dongwon Jeong, Kunsan National University, Korea

Technical Program Committee

Arno Puder, San Francisco State University, USA
Bin Xiao, Polytechnic University, Hong Kong
Cheng-Zhong Xu, Wayne State University, USA
Ho-Shin Cho, Kyungpook National University, Korea
Incheon Paik, The University of Aizu, Japan
Jung-Hong Chi, University of Connecticut, USA
Kiman Kim, Korea Maritime University, Korea
Kwangwoo Nam, Kunsan National University, Korea
Petr Hnetynka, University College Dublin, Ireland
Sangkyung Kim, Kangnung National University, Korea
Seong-Dong Kim, KETI, Korea
Sung-joon Park, Kangnung National University, Korea
Yonsik Lee, Kunsan National University, Korea
Zhou, Xiaobo, University of Colorado at Colorado Springs, USA

The Third International Workshop on RFID and Ubiquitous Sensor Networks (USN 2007)

Workshop Organizers

Young-Bae Ko, Kang-Won Lee

Workshop Description

Welcome to the proceedings of USN 2007, the Third International Workshop on RFID and Ubiquitous Sensor Networks. This workshop was a successor of USN 2006 held in Seoul, Korea, and it tried to bring together the recent advances in RFID and sensor technologies and the researchers who are active in the field and share interest in the area of ubiquitous sensor networks. This year's program covered a wide range of topics, including such issues as RFID tag anti-collision, security, target classification, and novel application development.

The exciting program is a result of the great support from all Program Committee members as well as a group of external reviewers. Taking this opportunity, we would like to thank all the Program Committee members and the reviewers for their hard work. We would also like to thank all the authors for their contributions to the program. We congratulate the authors of accepted papers, and regret that many quality submissions could not be included, due to the time limit of this program. We are also grateful to all the members of the Steering Committee for their advice and support. Finally, we would like to thank the EUC workshop Co-chairs, Mieso Denko and Chi-Sheng Shih, for the guidance in the organization of this workshop.

Workshop Co-chairs

Young-Bae Ko, Ajou University, Korea

Kang-Won Lee, IBM T.J. Watson Research Center, USA

Steering Committee

Jongsuk Chae, ETRI, Korea

Seung-Wha Yoo, Ajou University, Korea

Yu-Chee Tseng, National Chiao Tung University, Taiwan

Daeyoung Kim, Information and Communications University, Korea

Program Committee

Byunghun Song, KETI, Korea
Chansu Yu, Cleveland State University, USA
Chih-Yung Chang, Tamkang University, Taiwan
Dong-Kyun Kim, Kyungpook National University, Korea
Jae-Hyun Kim, Ajou University, Korea
Javier Gomez, National University of Mexico, Mexico
JP Vasseur, Cisco, USA
Kui Wu, University of Victoria, Canada
Ling-Jyh Chen, Academia Sinica, Taiwan
Mineo Takai, UCLA, USA
Ming-Jer Tsai, National Tsing-Hua University, Taiwan
Mischa Dohler, France Telecom, France
Mohamed Younis, University of Maryland, USA
Ozgur Ercetin, Sabanci University, Turkey
Saad Biaz, Auburn University, USA
Taekyung Kwon, Seoul National University, Korea
Tae-Jin Lee, Sungkyunkwan University, Korea
Yuh-Shyan Chen, National Chung Cheng University, Taiwan
Wei Lou, Hong Kong Polytechnic University, China
Wen-Chih Peng, National Chiao Tung University, Taiwan
Wonjun Lee, Korea University, Korea

The Second International Workshop on Embedded Software Optimization (ESO 2007)

Workshop Organizers

Shih-Hao Hung and Jun Wu

Workshop Description

As embedded systems are more pervasive in our everyday lives, they have become an active research topic in recent years. The increasingly ubiquitous embedded systems pose a host of technical challenges different from those faced by general-purpose computers because they are more constrained in terms of timing, power, area, memory and other resources. The optimization of embedded software becomes a major concern for embedded system design. The goal of ESO 2007 was to provide a forum for scientists, engineers, and researchers to discuss and exchange their new ideas, novel results, work in progress and experience on all aspects of embedded software optimization.

This year we received seven high-quality submissions. We conducted a rigorous peer-review process for each submission, with the great support of Program Committee members. Based on the reviews, we selected three papers to be included in this program. In addition, four quality papers from the main conference (EUC 2007) were invited to be presented in this workshop based on the recommendation of the reviewers. We congratulate the authors of accepted papers, and regret many quality submissions could not be included, due to the time limit of this program.

Taking this opportunity, we would like to thank all the authors for their contributions to the program. We are grateful that Tei-Wei Kuo (Program Chair of EUC 2007) and Chi-Sheng Shih (Co-chair of EUC 2007 Workshops) helped us with the invited papers and the publication matters. Finally, we would also like to thank the PC members for their efforts in reviewing the submissions.

Workshop General Co-chairs

Edwin H.-M. Sha, University of Texas at Dallas, USA
Sun-Yuan Kung, Princeton University, USA

Workshop Program Co-chairs

Shih-Hao Hung, National Taiwan University, Taiwan
Jun Wu, National Pingtung Institute of Commerce, Taiwan

Steering Committee Co-chairs

Edwin H.-M. Sha, University of Texas at Dallas, USA
Niraj K. Jha, Princeton University, USA
Tei-Wei Kuo, National Taiwan University, Taiwan
Laurence T. Yang, St. Francis Xavier University, Canada
Minyi Guo, University of Aizu, Japan

Program Committee

Ben A. Abderazek, Univ. of Electro-communications, Japan
Murali Annavaram, Nokia, USA
Tien-Fu Chen, National Chung Cheng University, Taiwan
Vipin Chaudhary, Wayne State University, USA
Yen-Kuang Chen, Intel, USA
Albert Cheng, University of Houston, USA
Alexander G. Dean, North Carolina State University, USA
Tony Givargis, University of California at Irvine, USA
Luis Gomes, Universidade Nova de Lisboa, Portugal
Houcine Hassan, Polytechnic University of Valencia, Spain
Seongsoo Hong, Seoul National University, Korea
Yuan-Shin Hwang, National Taiwan Ocean University, Taiwan
Zhiping Jia, Shangdong University, China
Ming-Haw Jing, I-Shou University, Taiwan
Sung-Yuan Ko, I-Shou University, Taiwan
Hsien-Hsin Lee, Georgia Institute of Technology, USA
Jeng-Kuen Lee, National Tsing Hua University, Taiwan
Yann-Hang Lee, Arizona State University, USA
Rainer Leupers, RWTH Aachen University, Germany
Xuandong Li, Nanjing University, China
Shih-Wei Liao, Intel, USA
Meilin Liu, Wright University, USA
Koji Nakano, Hiroshima University, Japan
Nicolas Navet, LORIA, France
Jogesh Muppala, Hong Kong Univ. of Science and Technology, Hong Kong
Gang Qu, University of Maryland, USA
Liang-Cheng Shiu, Nat'l Pingtung Inst. of Commerce, Taiwan
Jarmo Takala, Tampere University of Technology, Finland
Shao-Li Tsao, National Chiao Tung University, Taiwan
Karen A. Tomko, University of Cincinnati, USA
Lorenzo Verdoscia, ICAR, National Research Council, Italy
Bernhard Weiss, Vienna Inst. of Technology, Austria
Hongxing Wei, Beijing Univ. of Aero. & Astro., China

Wayne H. Wolf, Princeton University, USA
Jingling Xue, University of New South Wales, Australia
Chia-Ling Yang, National Taiwan University, Taiwan
Pen-Chung Yew, University of Minnesota, USA
Sheng-De Wang, National Taiwan University, Taiwan

The Third International Symposium on Security in Ubiquitous Computing (SecUbiq 2007)

Workshop Organizer

Laurence T. Yang, Zonghua Zhang, Jemal H. Abbawajy, Jong Hyuk Park, Deqing Zou, Emmanuelle Anceaume

Workshop Description

We are proud to present the proceedings of the Third International Symposium on Security in Ubiquitous Computing (SecUbiq 2007), held in Taipei, Taiwan during December 17–20.

The ubiquitous computing paradigm foresees seamless integration of communicating and computational devices and applications (e.g., smart sensors, wireless networks and mobile agents) embedded in all parts of our environment, from our physical selves, to our homes, our offices, our streets and so forth. Although ubiquitous computing presents exciting enabling opportunities, the benefits will only be realized if security issues can be appropriately addressed.

The overall aim of this symposium is to provide a forum for academic and industry professionals to discuss recent progress in methods and technologies concerning the identification of risks, the definition of security policies, and the development of security measures for ubiquitous computing.

In response to the call for papers, we received 38 papers from around the world including Korea, China, Hong Kong, Taiwan, Japan, Spain, Canada and USA, representing more than 20 universities and institutions.

In order to guarantee high-quality proceedings, we put extensive effort into reviewing the papers. All submissions were peer reviewed by at least three Program Committee members as well as external reviewers. As the quality of the submissions was quite high, it was extremely difficult to select the papers for oral presentations and publication in the proceedings of the symposium. After extensive discussion and based on the reviews, we finally decided to accept 11 papers for oral presentation and publication in the proceedings. We believe that the chosen papers and topics provide novel ideas, new results, work in progress and state-of-the-art techniques in this field as well as stimulate future research activities.

This symposium would not have been possible without the support of many people, who made it a success. First of all, we would like to thank the EUC 2007 workshop Chairs, Mieso Denko and Chi-Sheng Shih, and the Steering Committee Chair, Laurence T. Yang. In addition, we thank the Program Committee members and external reviewers for their excellent job in reviewing the submissions and thus guaranteeing the quality of the symposium under a very tight schedule. We are also indebted to the members of the Organizing Committee. Finally, we would like to take this opportunity to thank all the authors and participants for their contribution to making SecUbiq 2007 a grand success.

Symposium Committee

Steering Chair

Laurence T. Yang, St. Francis Xavier University, Canada

General Co-chairs

Zonghua Zhang, University of Waterloo, Canada

Jemal H. Abbawajy, Deakin University, Australia

Program Co-chairs

Jong Hyuk Park, Kyungnam University, Korea

Deqing Zou, Huazhong University of Science and Technology, China

Emmanuelle Anceaume, IRISA /CNRS, France

Program Committee

Leemon Baird, US Air Force Academy, USA

John T. Brassil, HP Laboratories, USA

Yuanshun Dai, Indiana University-Purdue University, USA

Arjan Durresi, Louisiana State University, USA

Huirong Fu, Oakland University, USA

Stefanos Gritzalis, University of the Aegean, Greece

Ligang He, University of Warwick, UK

Hanping Hu, Huazhong University of Science and Technology, China

Luis Javier García Villalba, Complutense University of Madrid, Spain

Hua Ji, Juniper Networks, USA

Zhiping Jia, Shandong University, China

Zhen Jiang, West Chester University, USA

ShiGuang Ju, Jiangsu University, China

Seungjoo Kim, Sungkyunkwan University, Korea

Raymond Li, CISCO, USA

Javier Lopez, University of Malaga, Spain

Sanglu Lu, Nanjing University, China

Jianhua Ma, Hosei University, Japan

Antonino Mazzeo, Second University of Naples, Italy

Jason A. Moore, US Air Force Academy, USA

Yi Mu, University of Wollongong, Australia

Yuko Murayama, Iwate Prefectural University, Japan

María S. Pérez-Hernández, Universidad Politécnica de Madrid, Spain

Xiao Qin, Auburn University, USA

Chunming Rong, University of Stavanger, Norway

Kouichi Sakurai, Kyushu University, Japan
Biplab K. Sarker, University of New Brunswick, Canada
Dino Schweitzer, US Air Force Academy, USA
Chi-Sheng (Daniel) Shih, National Taiwan University, Taiwan
Xinmei Wang, Xidian University, China
Yufeng Wang, Nanjing University of Posts and Telecommunications, China
Chuan-Kun Wu, Chinese Academy of Sciences, China
Liudong Xing, University of Massachusetts - Dartmouth, USA
Ming Xu, National University of Defence Technology, China
Jieh-Shan George YEH, Providence University, Taiwan
Hiroshi Yoshiura, University of Electro-Communications, Japan
Meng Yu, Monmouth University, USA
Ning Zhang, University of Manchester, UK
Xukai Zou, Indiana-Purdue University, USA

Table of Contents

Trustworthiness, Reliability and Services in Ubiquitous and Sensor Networks

| | |
|--|-----|
| Attack-Resilient Random Key Distribution Scheme for Distributed Sensor Networks | 1 |
| <i>Firdous Kausar, Sajid Hussain, Tai-hoon Kim, and Ashraf Masood</i> | |
| A Critical Approach to Privacy Research in Ubiquitous Environments – Issues and Underlying Assumptions | 12 |
| <i>Maria Karyda, Stefanos Gritzalis, and Jong Hyuk Park</i> | |
| The Case Study of Information Security System for International Airports | 22 |
| <i>Hangbae Chang, Moonoh Kim, Hyuk-jun Kwon, and Byungwan Han</i> | |
| Quantitative Evaluation of Intrusion Tolerant Systems Subject to DoS Attacks Via Semi-markov Cost Models | 31 |
| <i>Toshikazu Uemura and Tadashi Dohi</i> | |
| An Efficient Mutual Authentication Scheme for EPCglobal Class-1 Generation-2 RFID System | 43 |
| <i>N.W. Lo and Kuo-Hui Yeh</i> | |
| UPS – An Ubiquitous Proximity eService for Trust Collaboration | 57 |
| <i>Yuan-Chu Hwang and Soe-Tsyr Yuan</i> | |
| Obligations for Privacy and Confidentiality in Distributed Transactions | 69 |
| <i>U.M. Mbanaso, G.S. Cooper, David Chadwick, and Anne Anderson</i> | |
| Multi-channel Enhancements for IEEE 802.11-Based Multi-hop Ad-Hoc Wireless Networks | 82 |
| <i>YongSuk Lee, WoongChul Choi, SukJoong Kang, and SeongJe Cho</i> | |
| An Intelligent Event-Driven Interface Agent for Interactive Digital Contents in Ubiquitous Environments | 93 |
| <i>Sukhoon Kang and Seokhoon Bae</i> | |
| A Loop-Based Key Management Scheme for Wireless Sensor Networks | 103 |
| <i>YingZhi Zeng, BaoKang Zhao, JinShu Su, Xia Yan, and Zili Shao</i> | |
| A MAC Protocol with Little Idle Listening for Wireless Sensor Networks | 115 |
| <i>Chaoguang Men, Yongqian Lu, and Dongsheng Wang</i> | |

Security Technologies Based on Home Gateway for Making Smart Home Secure 124
Geon Woo Kim, Deok Gyu Lee, Jong Wook Han, and Sang Wook Kim

Layered Peer to Peer Streaming Using Hidden Markov Models 136
Sheng-De Wang and Zheng-Yi Huang

Optimum Power Controller for Random Number Generator in the Crypto Module of Ubiquitous Computing Environment 146
Jinkeun Hong and Kihong Kim

Problem Localization for Automated System Management in Ubiquitous Computing 158
Shunshan Piao, Jeongmin Park, and Eunseok Lee

System and Software for Wireless SoC

A High Speed Analog to Digital Converter for Ultra Wide Band Applications..... 169
Anand Mohan, Aladin Zayegh, and Alex Stojcevski

Design and DSP Software Implementation of Mobile WiMAX Baseband Transceiver Functions 181
Hai-wei Wang, David W. Lin, Kun-Chien Hung, and Youn-Tai Lee

Cross-Layer Design for IEEE 802.16-2005 System Using Platform-Based Methodologies 193
Li-chuan Tseng, Kuan-yin Chen, and ChingYao Huang

A Dynamic Frequency Allocation Scheme for IEEE 802.16 OFDMA-Based WMANs Using Hungary Algorithm 205
Shiann-Tsong Sheu, Chih-Chen Yang, and Hsu-Sheng Chang

Wireless Network Management System for WiMAX / Wi-Fi Mesh Networks 215
Li-Der Chou, Shih-Yao Cheng, Chien-Yi Li, and Shing-Kuang Chen

An Implementation of QoS Framework for Heterogeneous Networks 226
Chang-Yang Ho and Hsi-Lu Chao

An Energy-Efficient MAC Design for IEEE 802.15.4-Based Wireless Sensor Networks 237
Yu-Kai Huang, Sze-Wei Huang, and Ai-Chun Pang

A Cross-Layer Signaling and Middleware Platform for Multi-interface Mobile Devices 249
Yung-Chien Shih, Kai-Cheng Hsu, and Chien-Chao Tseng

| | |
|--|-----|
| Enhanced Sleep Mode Operations for Energy Saving in IEEE 802.16e | 261 |
| <i>Sixian Zheng, Kuo Chen Wang, Shiao-Li Tsao, and Pochun Lin</i> | |
| Enhanced Fingerprint-Based Location Estimation System in Wireless LAN Environment | 273 |
| <i>Wilson M. Yeung, JunYang Zhou, and Joseph K. Ng</i> | |
| Improving Channel Scanning Procedures for WLAN Handoffs | 285 |
| <i>Shiao-Li Tsao and Ya-Lien Cheng</i> | |

Network Centric Ubiquitous Systems

| | |
|---|-----|
| A Multicast Extension for Enhanced Mobile IP by Home Agent Handover | 297 |
| <i>Chun-Chuan Yang, Jeng-Yueng Chen, and Li-Sheng Yu</i> | |
| Autonomic Multi-server Distribution in Flash Crowds Alleviation Network | 309 |
| <i>Merdan Atajanov, Toshihiko Shimokawa, and Norihiko Yoshida</i> | |
| Generic Energy-Efficient Geographic Routing for Ad-Hoc Wireless Networks | 321 |
| <i>Chao-Lieh Chen, Jeng-Wei Lee, Cheng-Zh Lin, Yi-Tsung Chen, Jar-Shone Ker, and Yau-Hwang Kuo</i> | |
| Description of a New Feature Meta-model | 333 |
| <i>Yu Song and Qi Chen</i> | |
| Studying of Multi-dimensional Based Replica Management in Object Storage System | 341 |
| <i>Zhipeng Tan, Dan Feng, Fei He, and Ke Zhou</i> | |
| Communication Model Exploration for Distributed Embedded Systems and System Level Interpretations | 355 |
| <i>Takashi Kinoshima, Kazutaka Kobayashi, Nurul Azma Zakaria, Masahiro Kimura, Noriko Matsumoto, and Norihiko Yoshida</i> | |
| An End-to-End QoS Adaptation Architecture for the Integrated IntServ and DiffServ Networks | 365 |
| <i>Ing-Chau Chang and Shi-Feng Chen</i> | |
| Ubiquitous Laboratory: A Research Support Environment for Ubiquitous Learning Based on Sensor Networks | 377 |
| <i>Mianxiong Dong, Kaoru Ota, Minyi Guo, and Zixue Cheng</i> | |
| Intelligent Monitoring Using Wireless Sensor Networks | 389 |
| <i>Senol Zafer Erdogan, Sajid Hussain, and Jong-Hyuk Park</i> | |

| | |
|---|-----|
| On the Design of Micro-mobility for Mobile Network | 401 |
| <i>Junn-Yen Hu, Chen-Fu Chou, Min-Shi Sha, Ing-Chau Chang, and Chung-Yi Lai</i> | |
| ANSWER: Adaptive Network Selection in WLAN/UMTS EnviRonment | 413 |
| <i>Chih-Cheng Hsu, Ming-Hung Chen, Cheng-Fu Chou, Wei-Chieh Chi, and Chung-Yi Lai</i> | |
| Self-authorized Public Key Management for Home Networks | 425 |
| <i>Hyoungshick Kim and S. Jae Oh</i> | |
| A Cross-Layered Diagnostician in OSGi Platform for Home Network . . . | 435 |
| <i>Pang-Chieh Wang, Yi-Hsuan Hung, and Ting-Wei Hou</i> | |
| Ubiquitous Underwater Acoustic–Sensor Network | |
| LaMSM: Localization Algorithm with Merging Segmented Maps for Underwater Sensor Networks | 445 |
| <i>Eunchan Kim, Seok Woo, Chungsan Kim, and Kiseon Kim</i> | |
| TinyOS-Based Gateway for Underwater Acoustics/Radio Frequency Communication | 455 |
| <i>Phil-Jung Yun, Changhwa Kim, Sangkyung Kim, Seung-Jae Lee, and Yong-Man Cho</i> | |
| An Energy Scheduling Algorithm for Ensuring the Pre-determined Lifetime in Sensor Network | 467 |
| <i>Yong-Man Cho, Seung-Jae Lee, Changhwa Kim, and Sangkyung Kim</i> | |
| Underwater Acoustic Communication and Modem-Based Navigation Aids | 474 |
| <i>Dale Green</i> | |
| State-of-the-Art in MAC Protocols for Underwater Acoustics Sensor Networks | 482 |
| <i>Hung Trong Nguyen, Soo-Young Shin, and Soo-Hyun Park</i> | |
| An Ultrasonic Sensor Based Low-Power Acoustic Modem for Underwater Communication in Underwater Wireless Sensor Networks | 494 |
| <i>Heungwoo Nam and Sunshin An</i> | |
| UWA-NAV – Energy Efficient Error Control Scheme for Underwater Acoustic Sensor Network | 505 |
| <i>Soo-Young Shin and Soo-Hyun Park</i> | |

| | |
|---|-----|
| Underwater Wideband Source Localization Using the Interference Pattern Matching | 515 |
| <i>Seung-Yong Chun, Se-Young Kim, and Ki-Man Kim</i> | |
| A New Virtual Select Database Operation for Wireless Sensor Networks | 523 |
| <i>Seungjae Lee, Changhwa Kim, and Sangkyung Kim</i> | |
| GT ² – Reduced Wastes Time Mechanism for Underwater Acoustic Sensor Network | 531 |
| <i>Soo-Young Shin and Soo-Hyun Park</i> | |

RFID and Ubiquitous Sensor Networks

| | |
|--|-----|
| Comparative Evaluation of Probabilistic and Deterministic Tag Anti-collision Protocols for RFID Networks..... | 538 |
| <i>Jihoon Choi and Wonjun Lee</i> | |
| An Efficient Mutual Authentication Protocol on RFID Tags | 550 |
| <i>Hui-Feng Huang</i> | |
| HGLAP – Hierarchical Group-Index Based Lightweight Authentication Protocol for Distributed RFID System | 557 |
| <i>JeaCheol Ha, HwanKoo Kim, JeaHoon Park, SangJae Moon, Juanma Gonzalez Nieto, and Colin Boyd</i> | |
| Target Classification in Sparse Sampling Acoustic Sensor Networks Using IDDC Algorithm | 568 |
| <i>Youngsoo Kim, Daeyoung Kim, Taehong Kim, Jongwoo Sung, and Seongeun Yoo</i> | |
| Scriptable Sensor Network Based Home-Automation..... | 579 |
| <i>Thomas Haenselmann, Thomas King, Marcel Busse, Wolfgang E. elsberg, and Markus Fuchs</i> | |
| Applying Situation Awareness to Mobile Proactive Information Delivery | 592 |
| <i>SuTe Lei, Kang Zhang, and Edwin Sha</i> | |

Embedded Software Optimization

| | |
|---|-----|
| Energy-Efficiency on a Variable-Bitrate Device..... | 604 |
| <i>Yung-Hen Lee, Jian-Jia Chen, and Tei-Wei Kuo</i> | |
| The Secure DAES Design for Embedded System Application | 617 |
| <i>Ming-Haw Jing, Jian-Hong Chen, Zih-Heng Chen, and Yaotsu Chang</i> | |

| | |
|--|-----|
| Software Power Peak Reduction on Smart Card Systems Based on Iterative Compiling | 627 |
| <i>Matthias Grumer, Manuel Wendt, Stefan Lickl Christian Steger, Reinhold Weiss, Ulrich Ne e, and Andreas Mühlberger</i> | |
| Simultaneous Operation Scheduling and Operation Delay Selection to Minimize Cycle-by-Cycle Power Differential | 638 |
| <i>Wei-Ting Yen, Shih-Hsu Huang, and Chun-Hua Cheng</i> | |
| A Simple Approach to Robust Optimal Pole Assignment of Decentralized Stochastic Singularly-Perturbed Computer Controlled Systems | 648 |
| <i>Kai-chao Yao</i> | |
| Assured-Timeliness Integrity Protocols for Distributable Real-Time Threads with in Dynamic Distributed Systems..... | 660 |
| <i>Binoy Ravindran, Edward Curley, Jonathan S. Anderson, and E. Douglas Jensen</i> | |
| Evaluating Modeling Solutions on Their Ability to Support the Partitioning of Automotive Embedded Systems | 674 |
| <i>Augustin Kebemou and Ina Schieferdecker</i> | |
| Security in Ubiquitous Computing | |
| Security Analysis of the Certificateless Signature Scheme Proposed at SecUbiq 2006 | 686 |
| <i>Je Hong Park and Bo Gyeong Kang</i> | |
| New Efficient Certificateless Signature Scheme | 692 |
| <i>Lei Zhang, Futai Zhang, and Fangguo Zhang</i> | |
| A Practical Identity-Based Signature Scheme from Bilinear Map | 704 |
| <i>Zhu Wang and Huiyan Chen</i> | |
| Linkable Ring Signatures from Linear Feedback Shift Register | 716 |
| <i>Dong Zheng, Xiangxue Li, Kefei Chen, and Jianhua Li</i> | |
| A Simple and Efficient Key Exchange Scheme Against the Smart Card Loss Problem..... | 728 |
| <i>Ren-Chiun Wang, Wen-Shenq Juang, and Chin-Laung Lei</i> | |
| A Key Distribution Scheme Preventing Collusion Attacks in Ubiquitous Heterogeneous Sensor Networks | 745 |
| <i>Firdous Kausar, Sajid Hussain, Jong Hyuk Park, and Ashraf Masood</i> | |
| Token-Based Authenticated Key Establishment Protocols for Three-Party Communication | 758 |
| <i>Eun-Jun Yoon and Kee-Young Yoo</i> | |

| | |
|--|-----|
| Two Approaches on Pairwise Key Path Establishment for Sensor Networks | 770 |
| <i>Ping Li, Yaping Lin, and Jiaying Wu</i> | |
| An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks..... | 781 |
| <i>Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda</i> | |
| Low-Cost and Strong-Security RFID Authentication Protocol | 795 |
| <i>JeaCheol Ha, SangJae Moon, Juan Manuel Gonzalez Nieto, and Colin Boyd</i> | |
| A Ticket Based Binding Update Authentication Method for Trusted Nodes in Mobile IPv6 Domain | 808 |
| <i>Ilsun You</i> | |
| Author Index | 821 |

Attack-Resilient Random Key Distribution Scheme for Distributed Sensor Networks

Firdous Kausar¹, Sajid Hussain², Tai-hoon Kim³, and Ashraf Masood¹

¹ College of Signals, NUST, Rawalpindi, Pakistan
firdous.imam@gmail.com, ashrafm61@gmail.com

² Jodrey School of Computer Science, Acadia University, Nova Scotia, Canada
sajid.hussain@acadiau.ca

³ School of Multimedia, Hannam University, Daejeon, Korea
taihoonn@empal.com

Abstract. Key pre-distribution schemes are a favored solution for establishing secure communication in sensor networks. Often viewed as the safest way to bootstrap trust, the main drawback is seen to be the large storage overhead imposed on resource-constrained devices and also these schemes are quite insecure because pre-loading global secrets onto exposed devices strengthens the incentive for attackers to compromise nodes. To overcome these drawback, we propose a new key pre-distribution scheme for pairwise key setup in sensor networks. In our scheme each sensor node is assigned with small number of randomly selected generation keys instead of storing big number of random keys and a shared secret key can be efficiently computed from it. After generating the keys with neighbors the initial keys rings are being deleted from nodes memory. The analysis of our approach shows that it improves the previous random key pre-distribution schemes by providing the more resiliency against node capture and collusion attacks. Even if a node being compromised, an adversary can only exploit a small number of keys nearby the compromised node, while other keys in the network remain safe.

1 Introduction

A wireless sensor network typically consists of a potentially large number of incredibly resource constrained sensor nodes. Each sensor node is usually battery powered, and has a low-end processor, a limited amount of memory, and a low power communication module capable of short-range wireless communication. Their lifetime is determined by their ability to conserve power. The sensor nodes form an ad-hoc network through the wireless links. There are many technological hurdles that must be overcome for ad hoc sensor networks to become practical though. All of these constraints require new hardware designs, software applications, and network architectures that maximize the nodes capabilities while keeping them inexpensive to deploy and maintain. Wireless sensor networks are ideal candidates for a wide range of applications, such as target tracking and monitoring of critical infrastructures [1].

Secret communication is an important requirement in many sensor network applications, so shared secret keys are used between communicating nodes to encrypt data. Some of the major constraints like ad hoc nature, intermittent connectivity, and resource limitations of the sensor networks prevent traditional key management and distribution schemes to be applicable to WSN.

A typical WSN may contain from hundreds to thousands of sensor nodes. So any protocol used for key management and distribution should be adaptable to such scales. Sensor nodes in a WSN possess a unique communication pattern. Therefore, security protocols and most important the key management should take care of these patterns. A Berkeley Miac2 motes has a tiny Atmega Microprocessor and 128 KBytes of programmable flash memory. Hence, running computationally intensive cryptographic algorithms over such tiny embedded system devices is infeasible. Public key cryptography is therefore almost ruled out for serving security in WSNs. To avoid the use of public key cryptography, several alternative approaches have been developed to perform key management on resource-constrained sensor networks, such as random key pre-distribution schemes, plain text key exchange schemes, and transitory master key schemes.

Rest of paper is organized as follows. Section 2 provides the related work and Section 3 describes the Threat Model. Section 4 give the problem statement. In Section 5 proposed scheme is described. Section 6 gives the results and performance evaluation. Finally, Section 7 concludes the paper.

2 Related Work

The key management problem in wireless sensor networks has been studied in regard to different objectives and metrics. Eschenauer and Gligor [2] propose a distributed key establishment mechanism that relies on probabilistic key sharing among the nodes of a random graph and uses a shared-key discovery protocol for key establishment. Chan et al. further extend this idea and propose the q -composite key predistribution [3]. This approach allows two sensors to setup a pairwise key only when they share at least q common keys. Chan et al. also develop a random pairwise keys scheme to defeat node capture attacks. Leonardo B. Oliveira et al's [4] show how random key predistribution, widely studied in the context of flat networks, can be used to secure communication in hierarchical (cluster-based) protocols such as LEACH [5]. They present SecLEACH, a protocol for securing node-to-node communication in LEACH-based networks. These and some others [6,7,8,9,10] efforts have assumed a deployment of homogeneous nodes, and have therefore suggested a balanced distribution of random keys to each of the nodes to achieve security. Most of these schemes are suffered from high communication and computation overhead, and/or high storage requirement.

In [11] Perrig et al. propose SPINS, a security architecture specifically designed for sensor networks. In SPINS, each sensor node shares a secret key with the base station. Two sensor nodes cannot directly establish a secret key. However, they can use the base station as a trusted third party to set up the secret key.

Blundo et al. [12] propose several schemes which allow any group of t parties to compute a common key while being secure against collusion between some of them. These schemes focus on saving communication costs while memory constraints are not placed on group members. When $t = 2$, one of these schemes is actually a special case of Blom's scheme [13].

Availability of some information on the sensor distribution in the field helps to improve the security of the key pre-distribution schemes. Some location-aware schemes are proposed in [14] and [15]. These techniques divide the target field into non-overlapping square areas and randomly deploy the sensors in every area. The exact location of a sensor in any area is unknown, but there is knowledge about the identity of sensors in every area. This information helps to eliminate the dependency of keys between nonadjacent cells.

Du et al. [16] combine the key predistribution scheme of Blom [13] with the random key predistribution of [2] and propose a new scheme using multiple key spaces in which they first construct ω spaces using Blom's scheme, and then have each sensor node carry key information from τ (with $2 \leq \tau < \omega$) randomly selected key spaces. Two nodes can compute a shared key with high probability if they carry key information from a common space.

3 Threat Model

Sensor networks are often deployed in hostile environments, yet nodes cannot afford expensive tamper-resistant hardware. Therefore, a motivated attacker can compromise (via physical or remote exploitation) a set of nodes, obtaining their pairwise secret keys and controlling outbound communications. We also assume nodes can collude by sharing their keys with other attacker nodes. Traditionally, the threat from node compromise is measured by its impact on confidentiality, whether secret keys shared between uncompromised nodes can be obtained.

4 Problem Statement

In random key pre-distribution (RKP) schemes, a large pool of random symmetric keys and their ids is generated, and then every node is assigned with a number of keys randomly selected from a pool. After deployment, nodes broadcast ids of keys along with their node id to neighbors to determine their shared pairwise keys. If the network density, the size of the key pool, and the number of keys assigned to each sensor node are carefully chosen, then it can be ensured with high probability that all the neighboring nodes in the network will share at least one key with each other. While pre-distributing pairwise keys does protect confidentiality, it still loads nodes with a large number of globally-applicable secrets. By eliminating the eavesdropping attack, the pairwise scheme makes another type of malicious behavior more attractive. As several nodes possess the same keys; any node can make use of them. Simply combining the keys obtained from a significant number of compromised nodes greatly increases the attacker's chances of sharing keys with other nodes. A collusive attacker can share its

Table 1. Symbol Definition

| Notation Definition | |
|----------------------------|---|
| $f(m, k)$ | Pseudorandom function applying on message m using key k |
| $H(k, m)$ | One-way hash function applying on message m using key k |
| id_a | Identity of node N_a |
| R_a | Set of the keys in node N_a initial key ring |
| \acute{R}_a | Set of the keys in node N_a updated key ring |
| k_i^a | i -th key in node N_a key ring |
| k_i^{na} | i -th key in node N_a updated key ring |
| $K_{x,y}$ | A shared key between node N_x and N_y |
| \parallel | concatenation symbol |

pairwise keys between compromised nodes, enabling each to present multiple ‘authenticated’ identities to neighboring nodes while escaping detection [17]. In order to countering the collusion attacks, nodes should destroy unused keys from the node memory after an initialization phase, but this means new nodes can no longer join the system once initialization is complete.

5 Proposed Scheme

In this section we describe our key management scheme in detail. Table 1 shows the notation to be used latter.

Generate a key pool P consist of S different random keys which are called generation keys and their ids prior to network deployment. Shared pairwise keys are generated independently via these generation keys by applying a keyed hash algorithm on it. Before deploying the nodes, each node is loaded with its assigned key ring R which consist of m number of generation keys which are used as the generation knowledge of a number of keys.

For each node N_x , the assigning rules are as follows [18]. For every key $k_i \in P$ where $P = (k_1, k_2, \dots, k_S)$, compute $z = f(id_x, k_i)$; then, put k_i into R_x , the key ring of node N_x , if and only if $z \equiv 0 \pmod{\left(\frac{S}{m}\right)}$. This way we will fills R_x with m keys.

In the shared key discovery phase each node discovers its neighbor in wireless communication range with which it shares keys. The algorithm shown in Figure 1 will be executed on each node during shared key discovery phase. Each node broadcast its id to the neighboring nodes. The neighboring nodes which receive the message, compute the set of their key ids in order to find shared keys as follows. Consider a node N_a that is willing to know which keys it shares with its neighbors. It broadcast its id and wait to receive same broadcast message from neighboring nodes. Suppose it receive message from node N_b , it extract the node id from message i.e. id_b . For every key $k_j^a \in R_a$ node N_a computes $z = f(id_b, k_j^a)$. If $z \equiv 0 \pmod{\left(\frac{S}{m}\right)}$, it means that node N_b also has key k_j^a in its key ring i.e. $R_a \cap R_b = k_j^a$.

They will generate the shared pairwise key by applying keyed hash algorithm on id_a and id_b by using k_j^a , $K_{a,b} = H(k_j^a, id_a || id_b)$. After generating the shared keys with neighbors, each node destroy its initial key ring.

```

/* Initial State */
S: Key Pool
R: Key Ring
m: number of keys in key pool

procedure SharedKeyDiscovery()
1: broadcast( $id_a$ )
2: while receive=TRUE do
3:   packet=recieveBroadcastMsgs();
4:    $id_b$ =packet.getNodeId();
5:   for  $\forall k_j^a \in R_a$  do
6:      $z = f(id_b, k_j^a)$ 
7:     if ( $z \equiv 0 \pmod{\frac{S}{m}}$ ) then
8:        $K_{a,b} = H(k_j^a, id_a || id_b)$ 
9:     end if
10:  end for
11: end while

```

Fig. 1. Shared key discovery algorithm

5.1 Addition After Initial Deployment

Our approach should support the ability to allow new nodes to join network even after the nodes already present in the network has destroyed their initial key rings. The RKP scheme will be unable to add new nodes once the initial key rings has been deleted from node's memory. As a result, it is imperative that we develop a new solution capable of handling joins beyond the initial deployment. Suppose a newly joining node N_y wants to setup a pairwise key with an existing node N_x . There is a problem that how can N_x who no longer has its initial key ring can come to know that whether it shared any of its key from deleted key ring with N_y ?; We propose a solution that addresses this problems and allows new legitimate nodes to join an existing sensor network, while preserving opaqueness before and after erasure of node's key ring.

First, before a node N_x destroys its initial key ring, it generates a new key ring as shown in Figure 2. For every key k_i^x in its key ring, it generate a new key k_i^{nx} by applying pseudorandom function on its id and k_i^x . In this way it generate a set of new keys from keys in its initial key ring and assigned these newly generated keys the same id as that was of original keys in order to keep record that which keys it have in its initial key ring. Every new node join the network after initial deployment execute the algorithm shown in Figure 3 in order to discover the shared keys with neighbors.

```

procedure deleteKeyRing()
1: for  $\forall k_j^x \in R_x$  do
2:    $k_j^{n_x} = f(id_x, k_j^x)$ 
3:    $id_{k_j^{n_x}} = id_{k_j^x}$ 
4:   delete( $k_j^x$ )
5: end for

```

Fig. 2. Initial key ring update algorithm

```

procedure nodeAddition()
1: broadcast( $id_y$ )
2: while receive=TRUE do
3:   packet=recieveBroadcastMsgs();
4:    $id_x$ =packet.getNodeId();
5:   for  $\forall k_j^y \in R_y$  do
6:      $z = f(id_x, k_j^y)$ 
7:     if ( $z \equiv 0 \pmod{\frac{S}{m}}$ ) then
8:        $k_j^{n_x} = f(id_x, k_j^y)$ 
9:        $K_{x,y} = H(k_j^{n_x}, id_x || id_y)$ 
10:    end if
11:  end for
12: end while

```

Fig. 3. New node addition algorithm

Suppose new node N_y wants to join a network, it broadcast its node id (id_y) and wait for reply. When it receive reply message (say from node N_x), it extract node id. For every key $k_j^y \in R_y$ node N_y computes $z = f(id_x, k_j^y)$. If $z \equiv 0 \pmod{\frac{S}{m}}$, it means that node N_x also has key k_j^y in it initial key ring but it is no longer available now. So N_y computes corresponding key i.e. $k_j^{n_x}$ of N_x new key ring by applying pseudorandom function on id_x and k_j^y . Now they will generate the shared pairwise key by applying keyed hash algorithm on id_a and id_b by using $k_j^{n_x}$ i.e. $K_{x,y} = H(k_j^{n_x}, id_x || id_y)$.

6 Analysis

Earlier section described various steps in the proposed key management scheme. This section analyzes the algorithm as a whole to explain its features that make this scheme feasible to implement and better alternative option, compared to other similar key management algorithms.

To make it possible for any pair of nodes to be able to find a secret key between them, the key sharing graph $G_{ks}(V,E)$ needs to be connected. Given the size and the density of a network, how can we select the values for S and m , s.t., the graph G_{ks} is connected with high probability? We use the following approach, which is adapted from [2].

Let P_c be the probability that the key-sharing graph is connected. We call it global connectivity. We use local connectivity to refer to the probability of two neighboring nodes find at least one common key in their key rings. The global connectivity and the local connectivity are related: to achieve a desired global connectivity P_c , the local connectivity must be higher than a certain value; we call this value the required local connectivity, denoted by $p_{required}$.

Using connectivity theory in a random-graph by Erdos and Renyi, we can obtain the necessary expected node degree d (i.e., the average number of edges connected to each node) for a network of size n when n is large in order to achieve a given global connectivity, P_c :

$$d = \frac{(n-1)}{n} [\ln(n) - \ln(-\ln(P_c))] \quad (1)$$

For a given density of sensor network deployment, let \hat{n} be the expected number of neighbors within wireless communication range of a node. Since the expected node degree must be at least d as calculated above, the required local connectivity $p_{required}$ can be estimated as:

$$p_{required} = \frac{d}{\hat{n}} \quad (2)$$

After we have selected values for S and m , the actual local connectivity is determined by these values. Let p_s is the probability of any two neighboring nodes sharing at least one common key in their key rings

$$p_s = 1 - p'_s \quad (3)$$

Where p'_s , the probability that they will not share a key, is given by:

$$p'_s = \frac{[(S-m)!]^2}{S!(S-2m)!} \quad (4)$$

Knowing the required local connectivity $p_{required}$ and the actual local connectivity p_s , in order to achieve the desired global connectivity P_c , we should have $p_s \geq p_{required}$.

$$1 - \frac{[(S-m)!]^2}{S!(S-2m)!} \geq \frac{(n-1)}{n\hat{n}} [\ln(n) - \ln(-\ln(P_c))] \quad (5)$$

Therefore, in order to achieve a certain P_c for a network of size n and the expected number of neighbors for each node being \hat{n} , we just need to find values of S and m , such that Inequality (5) is satisfied.

We simulated a sensor network comprised of nodes uniformly distributed over a plane, setting $n = 1000$, $\hat{n} = 40$, and $P_c = 0.99$. In this setting the value of $p_{required}$ is 0.25. so we have to find the values of S and m such that $p_s \geq 0.25$. In Figure 4 we show the probability of key sharing i.e. p_s among nodes for different values of S and m .

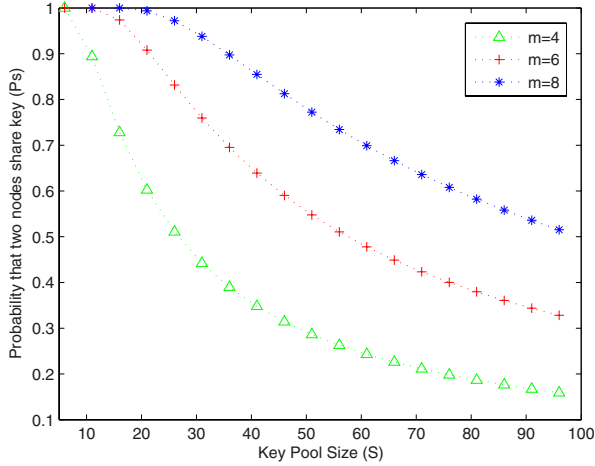


Fig. 4. The Key Sharing Probability

6.1 Security Analysis

We evaluate our key pre-distribution scheme in terms of its resilience against node capture and collusion attack.

Our evaluation is based on the metric that how much of network communication an adversary can compromise, when x nodes are captured. To compute this fraction, we first compute the probability that any one of the additional communication links is compromised after x nodes are captured. In our analysis, we are considering the links which are secured using a pairwise key computed from the common generation key shared by the two nodes of this link.

We should also notice that during shared key discovery process, two neighboring nodes find the common generation key in their key rings and use this key to agree upon another random key to secure their communication. Because this new key is generated from generation key by applying keyed hash algorithm on it, the security of this new random key does not directly depend on whether the key rings are broken. However, if an adversary can record all the communications during the key setup stage, he/she can still compromise this new key after compromising the corresponding links in the network. The fraction of communications compromised when x number of nodes being compromised is shown in Figure 5 in which we give the comparison of our proposed scheme (PS) with basic scheme (EG) and q -composite scheme.

Colluding attackers mainly take advantage of the pairwise secret keys stored by each sensor node as these keys are globally-applicable secrets and can be used throughout the network, yet ordinary sensors can only communicate with the small fraction of nodes within radio range. An attacker can readily exploit this lack of coordination between nodes and can now share its pairwise keys between compromised nodes, enabling each to present multiple ‘authenticated’ identities

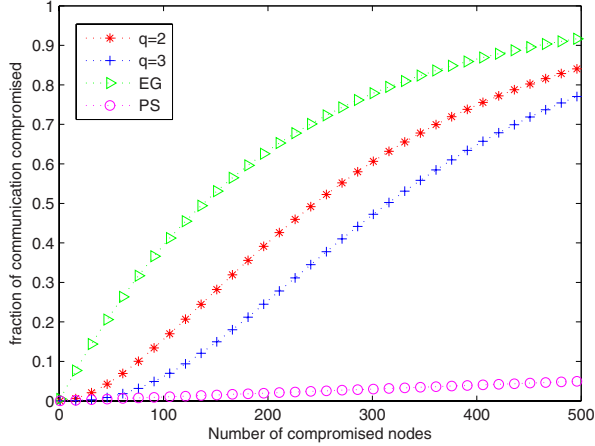


Fig. 5. The Compromising Probability

to neighboring nodes while escaping detection. In our proposed scheme we deleted the initial key ring from nodes memory after setting up shared pairwise keys with neighbors. Instead nodes generate a new key ring locally from initial key ring by applying one way hash function on node id and keys in its key ring. So no more globally-applicable secret remains in the node memory and it is not possible by adversary to launch this attack.

7 Conclusion

In this paper we proposed a key distribution scheme for wireless sensor networks which is secure against collusion attack. The analysis shows that the proposed scheme provides more resiliency against node capture and collusion attack by deleting the initial key rings from their memory after generating the shared pairwise key with neighbors. It also allows new nodes to join the system once initialization is complete and the initial key ring has been destroyed from the node's memory.

Acknowledgment

This work is in part supported by Higher Education Commission (HEC) Pakistan's International Research Support Initiative Program's scholarship given to Firdous Kausar to conduct her research at Acadia University, Canada, under supervision of Dr. Sajid Hussain. Further, the work was partly supported by Dr. Hussain's National Science and Engineering Research Council (NSERC) Canada's RTI and Discovery grants.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. *IEEE Communications Magazine* (2002)
2. Eschenauer, L., Gligor, V.D.: A key management scheme for distributed sensor networks. In: *ACM CCS* (2002)
3. Chan, H., Perrig, A., Song, D.: Random key pre-distribution schemes for sensor networks. In: *IEEE Symposium on Security and Privacy*, pp. 197–213 (2003)
4. Oliveira, L.B., Wong, H.C., Bern, M., Dahab, R., Loureiro, A.A.F.: Sec leach: A random key distribution solution for securing clustered sensor networks. In: *5th IEEE international symposium on network computing and applications*, pp. 145–154 (2006)
5. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: *IEEE Hawaii Int. Conf. on System Sciences*, pp. 4–7 (2000)
6. Chan, H., Perrig, A., Song, D.: Random key pre-distribution schemes for sensor networks. In: *IEEE Symposium on Research in Security and Privacy* (2003)
7. Zhu, S., Xu, S., Setia, S., Jajodia, S.: Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach. In: *ICNP 2003. 11th IEEE International Conference on Network Protocols* (2003)
8. Pietro, R.D., Mancini, L.V., Mei, A.: Random key assignment secure wireless sensor networks. In: *1st ACM workshop on Security of Ad Hoc and Sensor Networks* (2003)
9. Cheng, Y., Agrawal, D.P.: Efficient pairwise key establishment and management in static wireless sensor networks. In: *Second IEEE International Conference on Mobile ad hoc and Sensor Systems* (2005)
10. Ren, K., Zeng, K., Lou, W.: A new approach for random key pre-distribution in large-scale wireless sensor networks. *Wireless communication and mobile computing* 6(3), 307–318 (2006)
11. Perrig, A., Szewczyk, R., Tygar, J., Victorwen, Culler, D.E.: Spins: Security protocols for sensor networks. In: *Seventh Annual Int'l Conf. on Mobile Computing and Networks* (2001)
12. Blundo, C., Santis, A.D., Herzberg, A., Kutten, S., Vaccaro, U., Yung, M.: Perfectly-secure key distribution for dynamic conferences. In: Brickell, E.F. (ed.) *CRYPTO 1992. LNCS, vol. 740*, pp. 471–486. Springer, Heidelberg (1993)
13. Blom, R.: An optimal class of symmetric key generation systems. In: Beth, T., Cot, N., Ingemarsson, I. (eds.) *EUROCRYPT 1984. LNCS, vol. 209*, pp. 335–338. Springer, Heidelberg (1985)
14. Liu, D., Ning, P.: Location-based pairwise key establishments for static sensor networks. In: *SASN 2003. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pp. 72–82. ACM Press, New York (2003)
15. Wadaa, A., Olariu, S., Wilson, L., Eltoweissy, M.: Scalable cryptographic key management in wireless sensor networks. In: *ICDCSW 2004. Proceedings of the 24th International Conference on Distributed Computing Systems Workshops - W7: EC*, pp. 796–802. IEEE Computer Society, Washington, DC (2004)
16. Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J., Khalili, A.: A pairwise key predistribution scheme for wireless sensor networks. *ACM Trans. Inf. Syst. Secur.* 8(2), 228–258 (2005)

17. Moore, T.: A collusion attack on pairwise key predistribution schemes for distributed sensor networks. In: PERCOMW 2006. Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops, p. 251. IEEE Computer Society, Washington, DC (2006)
18. Pietro, R.D., Mancini, L.V., Mei, A.: Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks. *Wirel. Netw.* 12(6), 709–721 (2006)

A Critical Approach to Privacy Research in Ubiquitous Environments – Issues and Underlying Assumptions

Maria Karyda¹, Stefanos Gritzalis¹, and Jong Hyuk Park²

¹ Dept. of Information & Communication Systems Engineering, University of the Aegean, Greece

{mka, sgritz}@aegean.gr

² School of Computer Engineering, Kyungnam University, Masan-si, Kyungnam-do, Korea
parkjonghyuk@gmail.com

Abstract. This paper explores the different aspects of ubiquitous environments with regard to the protection of individuals' private life. A critical review of the relative research reveals two major trends. First, that there is a shift in the perception of privacy protection, which is increasingly considered as a responsibility of the individual, instead of an individual right protected by a central authority, such as a state and its laws. Second, it appears that current IT research is largely based on the assumption that personal privacy is quantifiable and bargainable. This paper discusses the impact of these trends and underlines the issues and challenges that emerge. The paper stresses that, for the time being, IT research approaches privacy in ubiquitous environments without taking into account the different aspects and the basic principles of privacy. Finally the paper stresses the need for multidisciplinary research in the area, and the importance that IT research receives input from other related disciplines such as law and psychology. The aim of the paper is to contribute to the on-going discourse about the nature of privacy and its role in ubiquitous environments and provide insights for future research.

Keywords: Ubiquitous Computing, Privacy Protection, Privacy Rights, Asymmetry of Power, Asymmetry of Information.

1 Introduction

Ubiquitous Computing (UC) refers to environments where most physical objects are enhanced with digital qualities. It implies that small, often tiny-sized devices with computing capabilities which are wirelessly interconnected are embedded almost invisibly into most objects used in everyday life. These devices can be anything from a device that only allows identification or positioning of the user to a fully featured mobile device that is capable of intense interaction with the user.

It has been suggested that security and privacy are among the major obstacles that do not allow the proliferation of ubiquitous applications. The concept of privacy is not new and can generally be defined as the individuals' ability to control the terms by which their personal information is collected and used. It is also widely acceptable

that privacy protection is of critical importance both at the individual and at the society level.

Although research on privacy in the area of ubiquitous computing expands in many different directions and covers various topics, privacy issues are still open and it appears that feasible and effective solutions are still quite far from being realized.

A critical analysis of current research on privacy in ubiquitous environments reveals that we are witnessing a significant change: up to now, it was the role of the government to provide the framework for privacy protection, as part of their role in the development of a welfare state for their citizens [1]; however lately there is a tendency to shift privacy protection into the hands of the individuals and to provide them with privacy protection mechanisms and tools. IT industry and related research have adopted the approach that end-users need to control information disclosure. Another finding, stemming from the analysis of relevant research, is that privacy is viewed as a quantifiable attribute that can be negotiated and possibly exchanged by individuals in return for certain benefits.

This paper examines these assumptions and explores their implications with regard to fair information practices. The aim of the paper is to contribute to the on-going discussion about privacy in the area of ubiquitous computing and to substantiate the importance of a multidisciplinary approach and the value of input from related fields.

The rest of the paper is structured as follows: Section two presents an overview of the field, focusing on the particular characteristics of ubiquitous environments and the basic principles for privacy and data protection. Section three identifies the major streams of research in ubiquitous computing with regard to privacy and section four discusses the implications of the underlying assumptions that prevail in privacy research. Finally, section five presents our conclusions and provides suggestions for future research.

2 Background

2.1 Characteristics of Ubiquitous Environments

A ubiquitous computing environment, also known as pervasive, is typically envisioned as a space populated with large number of invisible, collaborating computers, sensors and actuators interacting with user-held and/or user-worn devices. Ubiquitous environments comprise of hardware and software elements, as well as social or human elements since it is humans who receive services and interact with each other. Thus, ubiquitous environments span both the physical and the logical space. The physical space is the realm of the human staff, the devices and locations, whereas in the logical space actions are performed through the software. Up to now and by far, the vision of ubiquitous computing is mainly hardware-driven [2]. Research in software has also been active in the field, with research in smart agents and web services to prevail. The least researched into aspect of ubiquitous environments is the social one. The role of human principals in ubiquitous environments is primarily goal definition, preferences setting and strategies definition.

An important attribute for ubiquitous applications is *context awareness*. Context is a broad concept and is used to describe the physical, geographical, digital and social

surroundings of a smart device, as well as how it is being used by the user. In some cases, context may also include information on the biometrics of the user. Dey describes context as “*...any information that can be used to characterize situation*” and distinguishes among several types of context, the most important of which are location, identity, time and activity [3]. The author of [4] extends the concept of context, stating that it also means the *history* of all of these parameters. Context-awareness, in general, refers to the ability of computing systems to identify and adapt to their environmental context.

Another major characteristic of a ubiquitous environment is the dynamic nature of the use of services as well as the changes in the location. Furthermore, UC is characterized by the ability to learn from the past and to adapt services accordingly; thus computing systems are required to ‘remember’ and therefore store personal data [5].

2.2 Privacy

The right to privacy protection is considered critical for a democratic society and it is recognized as a fundamental right in all major international treaties and agreements on human rights [1]. Privacy has also been defined as the right “*to be left alone*” [6]. Generally, many different types of privacy have been identified, including bodily, territorial, communication and informational privacy. In a digital environment, privacy can be defined as the individuals’ ability to control the terms by which their personal information is collected and used. Under this perspective, privacy implies control over personal information. Privacy rights are recognized in relation to an identifiable individual. Up to now, the basic approaches that have been used to protect an individual’s privacy include the adoption of regulatory and technical means and their combination.

Privacy protection regulations can take different forms: Within the European Union (EU), privacy is protected according to the general EU Directive 95/46/EC on personal data protection. This Directive and its amendments regulate the collection, use and transfer of personal data, the rights data subjects can exercise and the obligations data controllers have. Compliance is monitored by independent public supervisory authorities. The United States has a different approach to personal privacy protection: Sector-specific laws are applied, each regulating a specific aspect, for instance, communications privacy, financial privacy etc. In most countries, independently of the type of the existing regulation of privacy, personal data protection is also pursued through self regulation. The EU Directive, for example, introduces the concept of “codes of conduct” that should be followed by organizations and trade associations. Other types of self regulation include use of standards, such as privacy enhancing technologies (PETs), and privacy seals, which are used by web sites to inform their visitors that their data will be treated according to certain data protection principles, as certified by the trust mark organization. Approaches to support privacy protection through the use of technical means primarily involve the use of some type of PETs [6].

The basic and most commonly accepted principles for respecting an individual’s privacy include the elements of *necessity*, *finality*, *transparency* and *proportionality*.

Necessity refers to the identification of purposes and benefits for identifying, or using personal information and also involves the considerations of possible alternatives. The principle of *finality* refers to the collection and use of personal data for specific and explicit purposes, which must be legitimate. The principle of *transparency* states that individuals should be aware of these purposes, as well as of the means used for the collection of their personal information; thus they should be *notified*. In some cases it is also supported that individuals should be able to *choose* (principle of choice) and give their *consent* (principle of consent) to the collection and use of their personal information. Finally, *proportionality* refers to the accordance between the types and extend of personal data that is collected and used with regard to the pursued objectives. In other words, personal data collected should be relevant and appropriate with the aims of the UC system. It should be noted that the concept of privacy is culture dependent and no universal agreement as to its content exists; however, among these privacy principles, *necessity* is the one that is the most generally accepted.

The paradigm of fair information practices, which is a regulatory paradigm defining how personal information should be collected and treated, includes *notice* of users, *choice* over how their personal information is used, the *right to access* collected information, reasonable *security* of the information and *accountability* of the collector's side [7]. The author of [8] proposes the following set of principles for guiding privacy-aware ubiquitous system design: (a) Notice: users should always be aware of what data is being collected; (b). Choice and Consent: users should be able to choose whether their personal data is used; (c) Anonymity and pseudonymity should apply when identity is not needed; (d) Security: different amounts of protection depending on the situation; and (e) Access and recourse: users should have access to data about them.

2.3 Privacy in Ubiquitous Environments

Ubiquitous computing is populated both by privacy enhancing technologies and privacy decreasing technologies. Privacy enhancing technologies, mainly based on encryption and anonymization techniques, allow prevention or reduction of identification. Sensors and RFID technology are prominent examples of the latter; for instance RFID tags embedded in badges, clothing or other objects can provide information on a person's movements and whereabouts. Ubiquitous sensor networks, combined with robust data mining techniques and the decreasing cost of information storage amplify the tracking and profiling capabilities of personal information collectors, thus augmenting privacy intrusion capabilities. As smart devices increasingly pervade public as well as private places, it is expected that individuals will implicitly create continuous streams of personal related information regarding their actions, preferences and locations.

Currently, major threats to privacy originate from personal data aggregation and the increasing strength and capacity of search engines. The amplitude of information sources and the potential to aggregate or combine these sources so as to create a person's profile are threatening individual privacy.

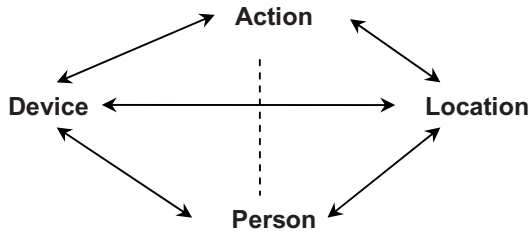


Fig. 1. The privacy diamond [9]

The privacy diamond shows [9], as depicted in Figure 1, that in ubiquitous environments (smart) devices operate between the individual and the information system or service provider. For this type of interaction to be realized some sort of identification is needed. Distinction should be made between devices that enable user request services from the system and devices that function automatically. Data collected are mainly personal data, or they can be easily transformed into personal data. This personal information gathered typically includes data with regard to the identity, location and activity of a person. In some cases, the device placed between the user and the information system or service provider can also be used to provide anonymous or pseudonymous access. However, it is the individuals who consciously request, or unconsciously launch, the collection of their personal data to receive services. It should also be noted that authentication between the device and the user is critical. However, due mainly to technical limitations (e.g. low computing power or lack of interaction ability) ubiquitous devices often do not support any authentication scheme.

In digital environments, deciding the level and type of required identification can be designed. However, in ubiquitous environments, the main question of how much identification is needed cannot be easily answered. The issue of whether, and which type of (personal) information is needed for the communication is not straightforward and depends on the situation. Generally, service providers depend on personal information to deliver personalized and location-based services. Thus, the everyday negotiation of privacy through interactive ubiquitous computing systems is considered an open issue.

To further discuss and comprehend the issue of privacy in the context of ubiquitous computing, we need to identify the stakeholders involved. In the first place, individuals, whose personal data are continuously monitored, collected and manipulated, are the major interested parties with regard to privacy protection. Other involved stakeholders include: IT industry, which provides the technical infrastructure and the privacy enhancing and privacy degrading tools; Organizations, or generally service providers that exploit the capabilities provided by ubiquitous computing to deliver services to individuals; and Governments, legal and regulatory authorities that provide the framework for privacy protection.

A major difficulty in the global digital environment where ubiquitous computing applications are realized is that the regulation approach based on legislation has very limited impact and thus limited effectiveness. Codes of conduct, on the other hand, present varying levels on effectiveness, based on the quality of their content, their

application context and the quality of enforcement and compliance monitoring schemes. Standardization efforts with regard to privacy protection are still at an early stage and could more appropriately be characterized as ‘recommendations’. Finally, the effectiveness of privacy seals is also difficult to be evaluated, since on line visitors as a rule lack the knowledge and necessary information to evaluate the protection provided by them.

It has been argued that privacy threats in ubiquitous environments are minimized due to the large number of devices in use, which make individual signals identification difficult. If millions of people use many different UC devices at home, on the road, at work or on their body, then the result will probably be “privacy by obscurity”. However, technically it is still achievable to filter information on a specific individual, especially if sophisticated technology is used. Thus, privacy remains an open issue, even if not as a generalized threat [2].

3 Streams of Privacy Research in Ubiquitous Computing

3.1 Digital Identities and Identity Management

In the physical world, identities distinguish one person from the other and are used as evidence for various purposes, such as access to services, authorizations, rights etc. For this reason, an identity typically comprises an aggregation of a person’s unique characteristics. On the logical sphere, the concept of ‘digital identity’ or ‘on-line identity’ or ‘virtual identity’ has emerged to connote personal data in digital form, such as, for example, usernames, passwords, tokens, PINs etc.). Digital identities are typically used in a similar way to physical ones: individuals receive services or are granted access, rights and privileges and according to their identity. However, in a digital environment individuals can have multiple digital identities, depending on their different roles. Consequently, a digital identity should not be equally treated or taken for granted as an identity in the physical world.

In ubiquitous environments, the digital identity is a concept mostly used to describe the appearance of a user, or a human entity. Such data are both generated by the infrastructure (for instance the MAC- or IP-address, which are automatically provided by the applications or the operating system) and the individual (e.g. by filling in forms with name and address, as well as other personal data, such as preferences). The “digital identity” is thus a construct of the receiver; the sender can only influence it by restricting the amount of personal data sent [2]. Virtual identities can be managed, created or abolished at the user’s will. Thus, virtual identities can be used as pseudonyms, and in this way function as privacy enhancing techniques due to their level of indirection between the real-world identity and the electronic data. It is generally known that opportunities to create fictitious virtual identities are highly exploited in the digital world not only for reasons of convenience and leisure, but also as a means to protect one’s privacy.

Identity management refers to the rules and procedures followed for manipulating different digital identities. Currently, many products and solutions are available on the market with regard to identity management: they provide different functionality ranging from provisioning and accounting, authentication, authorization to data consolidation.

3.2 Privacy Preserving Approaches

The “Platform for Privacy Preferences Project (P3P)” approach [10] specifies a privacy preserving architecture to be used by web sites that comprises user agents, privacy reference files, and privacy policies. Web sites that use the P3P platform announce their privacy practices to visitors and let them decide to accept or reject interaction. Within the P3P, the World Wide Web Consortium (W3C) provides guidelines that allow the encoding of privacy policies into XML, allowing automated processes to read such policies and take actions on them. The authors of [11] propose a general, component-based platform that functions as a middleware service that allows users apply general policies to control distribution of their information.

PawS [12] is a privacy awareness system for ubiquitous computing environments, which like P3P, provides users with tools in order to facilitate them protect their personal privacy. Its basis is primarily social and legal rather than technical. PawS uses privacy beacons that announce the privacy policies to user who enter an environment in which services are collecting data. Users’ privacy proxies, which act similarly to P3P’s user agents, check the announced policies, with regard to the user’s predefined privacy preferences. If the policies agree, users utilize the services and their information can be collected; if the policies are incompatible then users are notified by the system, and can choose their preferred course of action, which can vary from accepting or not the service, to leaving the area in which information collection is taking place.

Other approaches to privacy protection in ubiquitous environments include the use of the idea of trust systems and certification authorities that have been applied in other fields, such as Digital Rights Management (DRM), the concept of intermediate layers such as privacy proxies, the introduction of a ‘digital safe’ between citizens and public authorities as an alternative for traditional access rights, and the use of anonymity and pseudonymity. Finally, some researchers argue that privacy expectations vary [13] and depend on context [14].

In general, privacy research in ubiquitous computing is characterized by the belief that it is the individuals who are responsible, and thus should manage, their privacy and that privacy can be evaluated and exchanged, e.g. for the benefit of receiving customized, and thus higher-value services.

4 Discussion

Major research efforts in privacy protection with regard to ubiquitous environments adopt a decentralized approach, mainly by using some sort of middleware or proxy, that require the participation of the user, who has the ultimate responsibility to manage her privacy, be setting privacy preferences and by making decisions, automatically supported in most cases, on whether information practices are acceptable or not at each case.

This approach however, suffers the following limitations: it is very hard for the users to make an *informed choice*, since that would mean that they have full knowledge of technology, of the possible use of their personal data and its implications, as well as that they are aware of all their privacy rights. In digital

contexts, where asymmetry of information prevails, that is seldom the case. Moreover, even users had access to and the capability to comprehend all related information, their choice would not necessarily be free, since, they would possibly be declined access to certain services. This effect is called the *asymmetry of power*, and is usually experienced by users who employ some privacy enhancing technologies, for instance cookies blockage, to find out that they cannot have access to all web sites.

Another basic stream of privacy research in ubiquitous environments embraces the opinion that user perceptions of risk and benefit can determine their willingness to adopt technology. Multiple research endeavors explore the hypothesis that people are more likely to accept potentially invasive technology if they think its benefits will outweigh its potential risks [15, 16].

Privacy represents a sphere where it is possible to remain separate from others, anonymous and unobserved; thus it represents an aspect of freedom and, more specifically, freedom from interference [6]. The need for privacy emerges from within the society, from the various social relationships that people form with each other, with private sector institutions and with the government. Privacy is not merely a right possessed by individuals; it is a form of freedom built into the social structure [17].

If the right to privacy is treated as akin to property, meaning that privacy is *bargainable* and that it can be exchanged with other rights and privileges, then the element of individual dignity is totally ignored. However, dignity is inherent in the concept of privacy: dignity connotes the recognition of an individual's personality, respect for other people, non-interference with another's life choices and the possibility to act freely in society [18]. Human dignity, as source and expression of privacy, is not generated by the individual (it) "*is instead created by one's community and bestowed upon the individual. It cannot therefore be bartered away or exchanged*" [19].

Moreover, in ubiquitous environments the distinction between the private and the public sphere is blurred; fair information practices and legal frameworks for data protection have a point of reference; that is they apply in the public or the private sphere.

Since we have defined the concept of privacy as the individuals' ability to control the terms by which their personal information is collected and used, it is natural to draw the conclusion that privacy is closely related to the concept of *control*. However, in a dynamic and highly volatile environment, where individuals often maintain no direct physical contact with the computing devices, which may be tiny-sized, embedded and often difficult to be spotted, the span of a user's control over the information collected is generally very limited.

5 Conclusions

For Weiser's vision of ubiquitous computing to come true it is not only technology that needs to advance computing capabilities and blend them seamlessly into the fabric of every day life; close cooperation is needed among all stakeholders to resolve major privacy issues arising from the characteristics of the ubiquitous environment.

Managing privacy in the physical everyday life is a situated social process, and in most cases it is intuitively performed. People disclose different versions of personal

information to different parties under different conditions. However in the ubiquitous environment this issue is still not resolved, neither technically nor conceptually, meaning that there is not yet a clear and generally accepted idea of exactly privacy protection in a dynamic, pervasive environment means.

Up to now privacy research is dominated by a pure technical perspective, where the subtleties and deeper meanings and implications technology can have are not further examined. This paper has provided a critical analysis of research in the field of UC privacy, aiming to bring in the foreground hidden assumptions and discuss their implications. Our analysis of current research approaches has revealed two underlying assumptions which are commonly and unquestionably accepted by IT researchers: first, that privacy protection is the user's responsibility and second that privacy is considered 'bargainable' and 'quantifiable'. The main implication of these assumptions is that the protection of individual privacy in ubiquitous environments is envisioned that can be managed, even exchanged, in a distributed and measurable way; this, however, contradicts with the fundamental privacy and data protection principles that are currently supported. For this reason, this paper has argued that there is an imperative need that privacy research with regard to ubiquitous applications is informed and enriched with insight from other related fields, for instance law and psychology. Thus, a multidisciplinary approach is needed; researchers need to be informed about the different facets of privacy so as to make informed choices when exploring, designing or evaluating privacy protection schemes to be applied in the context of ubiquitous environments.

Acknowledgments

Jong Hyuk Park's research work was supported by Kyungnam University, Korea.

References

1. Dumortier, J., Goemans, C.: Roadmap for European Legal Research in Privacy and Identity Management, Interdisciplinary Centre for Law and ICT (ICRI), K.U. Leuven (December 2002)
2. Eymann, T., Morito, H.: Privacy Issues of Combining Ubiquitous Computing and Software Agent Technology in a Life-Critical Environment. In: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (2004)
3. Crowley, J.L., Coutaz, J., Rey, G., Reigner, P.: Perceptual Components for Context Aware Computing. In: Borriello, G., Holmquist, L.E. (eds.) UbiComp 2002. LNCS, vol. 2498, Springer, Heidelberg (2002)
4. Persson, P.: Social Ubiquitous Computing. In: Workshop on Building the Ubiquitous Computing User Experience, ACM/SIGCHI, Seattle (2001)
5. Čas, J.: Privacy in Pervasive Computing Environments – A Contradiction in Terms? IEEE Technology and Society Magazine, 24–33 (Spring 2005)
6. Grizalis, S.: Enhancing Web Privacy and Anonymity in the Digital Era. Information Management and Computer Security 12(3), 255–288 (2004)
7. Center for Democracy and Technology, Fair Information Practices, <http://www.cdt.org/>

8. Langheinrich, M.: Privacy by design – principles of privacy-aware ubiquitous systems. In: Abowd, G.D., Brumitt, B., Shafer, S. (eds.) *UbiComp 2001*. LNCS, vol. 2201, pp. 273–291. Springer, Heidelberg (2001)
9. Zugenmaier, A.: *Anonymity for Users of Mobile Devices through Location Addressing*. Rhombos Verlag, Berlin (2002)
10. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, World Wide Web Consortium (September 2001), <http://www.w3.org>
11. Miles, G., Friday, A., Davies, N.: Preserving Privacy in Environments with Location-Based Applications. *Pervasive Computing*, 56–64 (2003)
12. Langheinrich, M.: A Privacy Awareness System for Ubiquitous Computing Environments. In: Borriello, G., Holmquist, L.E. (eds.) *UbiComp 2002*. LNCS, vol. 2498, pp. 237–245. Springer, Heidelberg (2002)
13. Jiang, X., Hong, J.I., Landay, J.A.: Approximate Information Flows: Socially Based Modeling of Privacy in Ubiquitous Computing. In: Borriello, G., Holmquist, L.E. (eds.) *UbiComp 2002*. LNCS, vol. 2498, pp. 176–193. Springer, Heidelberg (2002)
14. Kobsa, A., Schreck, J.: Privacy through Pseudonymity in User-Adaptive Systems. *Transactions on Internet Technology* 3(2), 149–183 (2003)
15. Beckwith R.: Designing for Ubiquity: The Perception of Privacy. *Pervasive Computing*, 40–46 (April-June 2003)
16. Hann, I., Hui, K., Lee, T., Png, I.: Online Information Privacy: Measuring the Cost-Benefit Trade-Off. In: *Proc. of the 23rd International Conference on Information Systems* (2002)
17. Solove, D.J.: A taxonomy of privacy. *University of Pennsylvania Law Review* 154(3), 477–564 (2006)
18. Rodota, S.: Privacy, freedom and dignity – Closing remarks at the 26th International Conference on Privacy and Personal Data Protection, Wroclaw (16.09.2004)
19. Lasprogata, G., King, N., Pillay, S.: Regulation of Electronic Employee Monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada, *Stanford Technology Law Review*, 4 (2004), http://stlr.stanford.edu/STLR/Article?04_STLR_4

The Case Study of Information Security System for International Airports

Hangbae Chang¹, Moonoh Kim², Hyuk-jun Kwon³, and Byungwan Han⁴

¹ Daejin University,

San 11-1 Sundan Dong, Pocheon Si, Gyonggi Do, 487-711, Korea
hbchang@daejin.ac.kr

² Yonsei University

134 Sinchon-Dong, Seodaemun-Gu, Seoul, 120-749, Korea
perrang2@yonsei.ac.kr

³ Yonsei University

134 Sinchon-Dong, Seodaemun-Gu, Seoul, 120-749, Korea
junkwon@yonsei.ac.kr

⁴ Tongwon College

Sinchon Ri, Silchon Eup, Gwanju-Si, Gyonggi Doul, 464-711, Korea
bwhan@tongwon.ac.kr

Abstract. With continuing security concerns for airport operations, the protection of internal operational protocols of an international airport has become more critical than ever before. Therefore, the Information Security System (ISS) was developed for Incheon International Airport which can protect the critical information related to airport operations. The developed ISS includes a document access control server/client agent, a user access control service linker, and an operational log file database. The ISS was developed in consideration of information life cycle of airport workflow. As a result, it can securely protect the computer system at Incheon International Airport by (1) performing real-time encoding of the users who accessed the protected files and folders, (2) limiting the user's capability to edit the protected documents, (3) tracking transmitted files to the outside companies, (4) blocking the user's access to portable storage devices, and (5) inserting security water marks on the printed outputs. With the implementation of the ISS, the real-time information system audit environment has been securely established at the Incheon International Airport Corporation.

1 Introduction

Construction of the Incheon International Airport (IIA) was completed in December 2000 and its design is shown in Fig. 1. with two major runways and a passenger terminal of 496,000m². Recently, the IIA was selected as the best airport worldwide by ACI and IATA in 2005 [1]. Airport security can be classified into two categories: facility security and computer security. The physical facilities of the IIA are well protected by the airport security force that is in charge of the fences around the

airport, passenger terminal, transportation center, auxiliary facilities and free economic zone. The computer information security system has become more complex because most corporations like Incheon International Airport Corporation (IIAC) uses an integrated information system which shares information through intranet, groupware, knowledge management system and electronic document management system. This paper focuses on the computer information security system which would not only protect the information on the airport operations from outsiders but also prevent the internal employees from illegally releasing the protected information to the outsiders.



Fig. 1. Design of the Incheon International Airport

Although the construction and operation of the Incheon International Airport can be considered a very successful one, there are some areas in the corporate information security which can be improved.

- Lack of response plan for emergency: There are several emergency scenarios for the airport facilities but there is a lack of the security and response plan for emergency failure of the computer system.
- Lack of integration of emergency response systems: The current emergency response system at IIA are not well integrated and for an emergency situation such as illegal entry or fire through the electronic CAD drawings to locate the point of emergency, integration of CCTV and sensors, and broadcasting system to announce the emergency and evacuation plan.
- Lack of protection of corporate information: The critical information such as various internal documents and CAD drawings of the IIA facilities are not well protected and can be accessed and released to the outsiders by the malicious internal employees.

Recently, as reported in the Chosun newspaper on November 25th 2005, there was an incident at IIA which involved an internal employee who illegally accessed and released the design documents for the system integration project of IIA valued over \$150 million. This project was to integrate the security system, the communication system and the airport information system. The internal employee accessed the 250 related documents for the bidding purpose, saved them in CD and supplied it to a company who is interested in winning this security system integration project. This

information apparently would have given an advantage to this company over other competitors. The internal employee was later arrested by the police and this incident was considered a clear sign of computer system vulnerability to the internal intrusion at IIA. Such an internal security breach is more damaging than the external security breach because the internal employee is more knowledgeable with the computer system at IIA. This paper focuses on the development of the computer information security protection software and its implementation at IIA.

2 Corporate Information Protection Methods

As discussed earlier, the critical corporate knowledge can be leaked out by internal users in a number of ways. In this section, various knowledge protection methods are discussed [2].

As the information technology evolves, it has become easier to share and distribute the electronic CAD files leading to the efficient and collaborative design environment. However, the recent collaborative software such as DBMS (Data Base Management System), PMIS (Project Management Information System), KMS (Knowledge Management System) made CAD data more difficult to secure. If the CAD files fall into the competitor's hands by internal users, the engineering company will lose its competitive advantage over its competitors [3]. Therefore, it is critical to secure the CAD files so that such valuable intellectual property is not lost to competitors. In this section, we present studies of securing CAD files against illegal piracy of design knowledge after literature reviews.

2.1 Device Control Technology

The device control technology addresses the channel of knowledge leakage through portable storage devices such as USB memory device, CD, and DVD. Since this technology controls a variety of devices installed on the PC, it is difficult to implement such a restrictive security policy on a corporate-wide basis. Besides, it is nearly impossible to control all such possible hardware devices without negatively affecting the productivity. As a result, this device control technology can be applied to the limited number of internal users dealing with simple tasks.

2.2 Document Security Technology

The document security technology restricts discreet use of documents by controlling software packages used for preparing such documents such as Notepad, Word and Excel and enabling the management of the documents according to user authority. This technology can be applied to simple documents such as web pages and image files with a single extension.

2.3 Policy and Contract Approach

For the ultimate security of corporate knowledge, a contract like a non-disclosure agreement should be signed by everyone including the internal staff, collaborating

companies, suppliers and customers. This contractual protection of the corporate knowledge will give a clear message to all parties that the legal action will be pursued upon illegal handling of the confidential files.

3 Computer Security Protection System Development

As shown in Fig. 2, during a typical flow of the information in its life-cycle from creation to delivery, security holes can be identified as follows [2]:

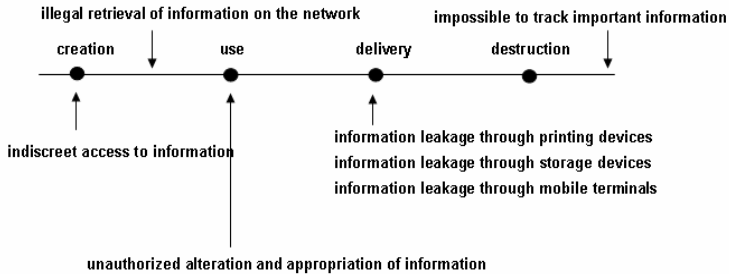


Fig. 2. Identification of security holes throughout the life cycle of information

- Indiscreet access to information: Without the access control system for newly created information, anybody may access the information indiscreetly. Then the value of information is diminished and the potential of information leakage is high.
- Unauthorized alteration and appropriation: Without the document security system, the information can be altered, misappropriated and misused by anybody.
- Indiscreet leakage of information: Without the device control system, the information can be distributed through the printing devices, portable storage devices and mobile terminals.
- Impossible to track important information: Without the document tracking system, it is difficult to track those who are involved in the information leakage and make them accountable for the damages caused by the information leakage.

3.1 Real-Time Encryption of User Files and Folders

As shown in Fig. 3, information created by users must be encrypted selectively or compulsorily according to the corporation's information security policy. If a separate security folder is designated and the access right policy is defined, all information stored in the security folder should be encrypted automatically. In addition, information in the subfolders of the security folder should be encrypted in the same way. Information copied or moved to other folders should remain as encrypted. The standard documents stored in the central computer server should be controlled by an individual user's access level[3, 6].

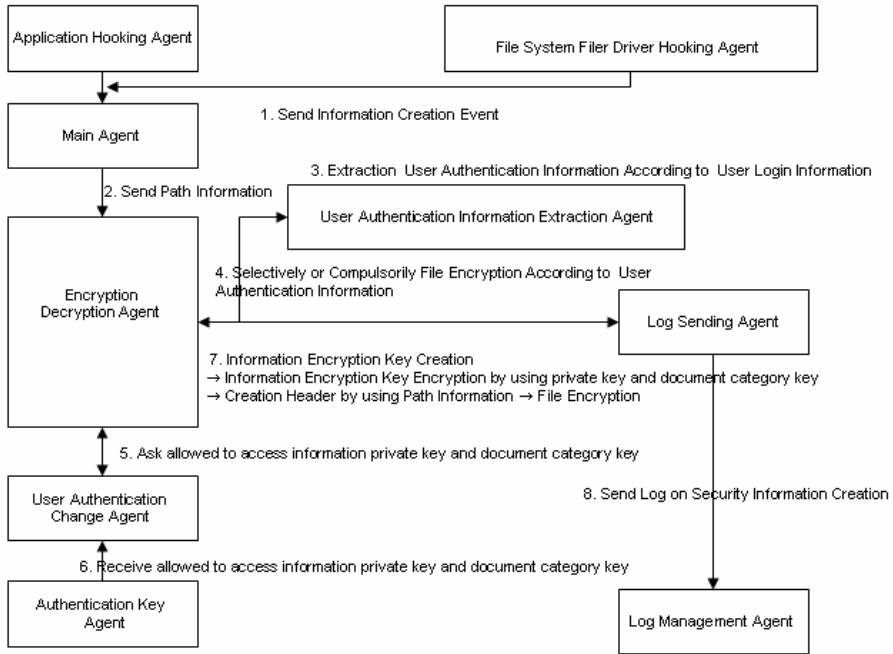


Fig. 3. Process of real-time encryption of user files and folders

3.2 Real-Time Authentication of User’s Access Right

All users should be given appropriate levels of access right depending on their status within corporation with respect to reading, editing, printing, releasing, effective date, and auto destruction. The user authentication should be performed in a real-time to verify his/her level of access right. When multiple users at different levels of access right collaborate on the same project, the original data used to create information should be protected separately.

3.3 Watermarking to Printouts

When the confidential information is printed, all printouts should contain watermarking so that printing activities can be monitored. The image of the output should be then sent to the management server which would record the document ID, the staff ID who printed and the time of printing and show on the output.

3.4 Security Code to Mobile Storage Devices

The information security protection system can apply a lock on all files created by a user but it will be cumbersome for a user to unlock all of his files most of which may not be considered confidential. Therefore, it is difficult to prevent an internal user who originally created the document without a security protection from copying it into his mobile storage devices such as floppy disks, USB memory disks, CD-RW,

and PDA. To prevent an illegal release of the confidential document through such external devices, it is necessary for the corporation to limit a user from using his/her personal devices. The information security system should assign the security code to all external devices including as laptop computers.

3.5 Security File for Outside Transmission

Although it is possible to control the document among internal users, when collaborating with people external to the corporation, it is not possible to share the encrypted files. Therefore, a user authentication and his/her access control level should be transmitted along with the encrypted file in the form of the executable file format. When the external user runs the executable file the file can be accessed without installing a separate program in his computer. For external (or internal) users, the file will be preset with the maximum allowed number of access along with the expiration date. If the external user tries to use the file after exceeding the allowed number of access in an allowed time period, the file will be automatically destroyed.

4 Implementation of Information Security System

The developed Information Security System (ISS) was implemented in the computer system at the Incheon International Airport Corporation, which is running Hand Software Groupware under Windows XP environment. As shown in Fig. 5. and 6, when a user log into the computer system, according to the access control policy, the user will be provided with the appropriate level of access control. The user will be then continuously monitored and controlled by the ISS. The standard operational documents within Incheon International Airport Corporation (IIAC) are classified as confidential and the access to these corporate documents is controlled by the ISS. Depending on a user's access rights, he/she can modify the corporate documents. If a user tries to access the file without an appropriate level of authority, he/she will be provided with the encoded message with a warning[5, 8, 10].

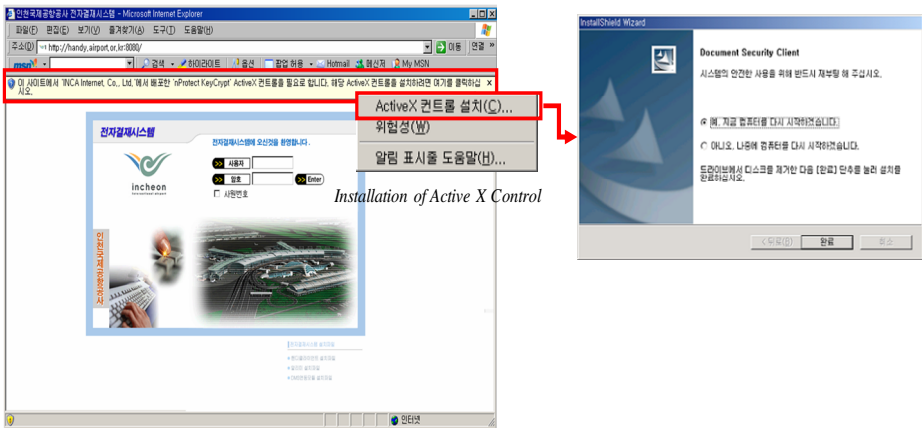


Fig. 4. Installation of Information Security System at IIAC



Fig. 5. System Level Protection of Corporate Documents

When the encoded document is to be transmitted to the outside, the encode file and the access right of the external user are transmitted in an executable file format. As shown in Fig. 6, in order to create an externally transmittable file, an internal user must click on the right button on the mouse and create the external user’s right and his/her password to open the file. The information security system automatically converts the file into executable file such as “document1.exe”. When the external user clicks on the exe file and enters his/her supplied password, the file will be open with a designated level of access right.

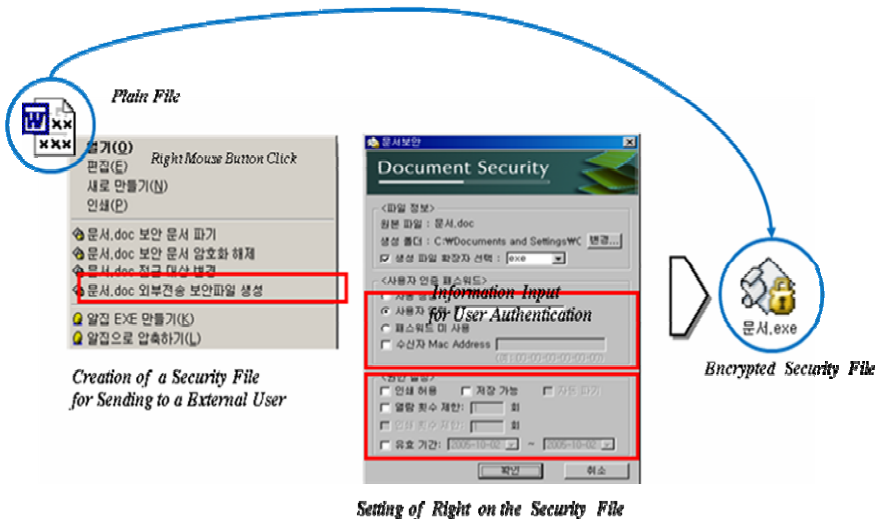


Fig. 6. Creation of Executable File for the Transmission to Outside

Finally, when the confidential document is printed, the information on the user is automatically printed on the output. As can be seen from Fig. 7, the basic watermarking of the IIAC logo, user ID, time of printing will be displayed on the printout. This

will alert the user about his/her identity is being disclosed not only to his/her corporation but also to whomever the output is provided.

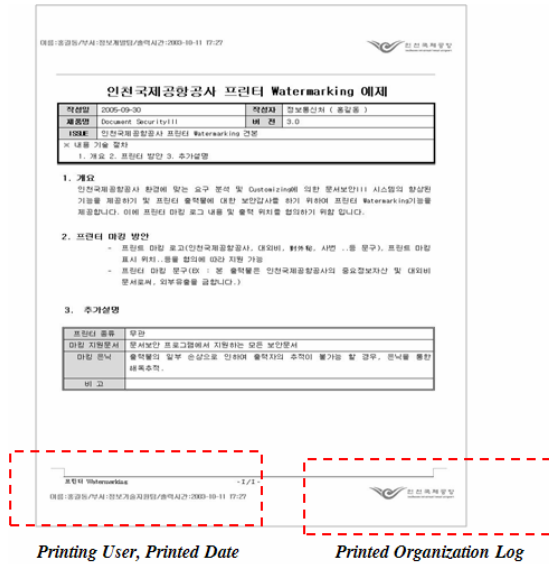


Fig. 7. Print Water Marking

5 Summary and Conclusion

The Information Security System (ISS) was developed and implemented at the Incheon International Airport Corporation (IIAC) where over 1,000 employees share numerous documents in the file formats of doc, xls, ppt, gif, bmp, pdf, txt, zip, and dwg. The ISS presented in this paper not only would provide the secure environment for sharing information at IIAC but also efficient working environment without unnecessary interruptions. Once the airport information security is compromised, the ISS will quickly detect and track down the source of such information leakage.

The information leakage points are identified and used to design the ISS to prevent such leakage. The ISS is designed to prevent the information leakage by deploying (1) real-time user authentication and user file and folder encoding technology, (2) external memory device and printing device control through water marking technology (3) external transmission control of the internal document by creating the executable file with security information.

The proposed ISS include a number of security control features which would not only stop the illegal access to the valuable corporation information but also track down if such an illegal access has taken place. However, when all of these security control functions are implemented, users may find the ISS constantly interfering with their daily job functions. Therefore, in the future, the proposed ISS should be expanded to become a virtual file system which can protect the confidential corporate information including the intermediate and temporary files.

Acknowledgement

"This research is supported by the ubiquitous Computing and Network (UCN) Project, the Ministry of Information and Communication (MIC) 21st Century Frontier R&D Program in Korea."

References

1. IIAC Newsletter, Issue 60 (May 2006)
2. Otwell, K., Aldridge, B.: The Role of Vulnerability in Risk Management. In: IEEE Proceedings of the 5th Annual Computer Security Applicant Conference, pp. 32–38 (1989)
3. Wagner, G.: Agent-Oriented Analysis and Design of Organizational Information Systems. In: Proc. of Fourth IEEE International Baltic Workshop on Databases and Information Systems, Vilnius (Lithuania) (May 2000)
4. Weiser, M.: The Computer for the 21st Century. *Scientific American* 265(3) (September 1991)
5. Suematsu, Y., Takadama, K., Nawa, N., Shimohara, K., Katai, O.: Analyzing levels of the microapproach and its implications in the agent-based simulation. In: Proceedings of the 6th International Conference on Complex Systems, Chuo University, Tokyo, Japan, pp. 44–51 (September 2002)
6. Wagner, G.: The Agent-Object-Relationship metamodel: Towards a uni-fied conceptual view of state and behavior. Technical report, Eindhoven Univ. of Technology, Fac. of Technology Management, Information Systems (May 2002), <http://AOR.research.info>
7. Bellifemine, F., Poggi, A., Rimassa, G.: Developing Multi-agent Systems with JADE. In: Castelfranchi, C., Lespérance, Y. (eds.) ATAL 2000. LNCS (LNAI), vol. 1986, pp. 89–103. Springer, Heidelberg (2001)
8. Bergenti, F., Poggi, A.: Ubiquitous Information Agents. *International Journal of Cooperative Information Systems* 11(3-4), 231–244 (2002)
9. Ayesh, A., Bechkoum, K.: Framework of multi-agents internet security system. In: AI 2000. *Appl Inform* (2000)
10. Lalana, K., Tim, F., Anupam, J.: Developing secure agent systems using delegation based trust management. In: Falcone, R., Barber, S., Korba, L., Singh, M.P. (eds.) AAMAS 2002. LNCS (LNAI), vol. 2631, Springer, Heidelberg (2003)

Quantitative Evaluation of Intrusion Tolerant Systems Subject to DoS Attacks Via Semi-Markov Cost Models

Toshikazu Uemura and Tadashi Dohi

Department of Information Engineering, Graduate School of Engineering
Hiroshima University
1-4-1 Kagamiyama, Higashi-Hiroshima, 739-8527 Japan

Abstract. In this paper we quantitatively evaluate the security of intrusion tolerant systems with preventive maintenance subject to DoS (Denial of Service) attacks. More specifically, we develop two semi-Markov cost models and describe the stochastic behavior of two intrusion tolerant systems with different preventive maintenance policies. The optimal preventive maintenance schedules are analytically derived to minimize the long-run average costs. We further perform the sensitivity analysis of the model parameters through numerical experiments. The results obtained here would be also useful to design ubiquitous systems subject to external malicious attacks.

Keywords: DoS attack, information security, intrusion tolerance, preventive maintenance, long-run average cost, semi-Markov models.

1 Introduction

Recently, since a huge number of information systems are connected by public network like internet and can be accessed by many unspecified people, we often encounter the serious problems on accidental and malicious threats. Once the security intrusion happens, it may lead to not only the leak/destruction of information but also the computer system down. For malicious attackers, if the access right strengthens, the probability that the security intrusion happens will decrease, but the utilization on accessibility will be rather lost. Hence, when the information security systems are designed, it is quite important to take account of both intrusion detection function and intrusion tolerant function. The former strengthens the access right against malicious accesses, the latter tolerates the security intrusion at the minimum risk. In fact, a number of implication techniques of intrusion tolerance at the architecture level have been developed for several real systems [13], [14], *e.g.*, distributed systems [1], middleware [15], database systems [16], server systems [3]. The above approaches are based on the redundant design at the architecture level on secure software systems. In other words, these methods can be categorized by a design diversity technique in secure system design and need much cost for the development. On the other hand, the environment diversity technique by the temporal time redundancy is a low-cost

security tolerance technique. The most plausible examples for applying the environment diversity technique are ubiquitous systems under unspecified operation environment. In this paper we focus on the security design of intrusion tolerant systems with preventive maintenance.

The quantitative evaluation of information security based on modeling is quite effective to validate the effectiveness of information systems with intrusion tolerance. Littlewood et al. [6] found the analogy between the security theory and the traditional reliability theory in assessing the quantitative security of operational software systems and proposed some quantitative security measures. Jonsson and Olovsson [5] discussed a quantitative method to study the attacker's behavior with the empirical data observed in experiments. Ortalo, Deswarte and Kaaniche [9] applied the privilege graph and the Markov chain to evaluate the vulnerability, and derived the mean effort to security failure. Singh, Cukier and Sanders [11] and Stevens et al. [12] considered probabilistic models to verify the intrusion tolerant systems against several attack patterns, and explained theoretically the detection mechanism of system vulnerability. Madan et al. [7], [8] dealt with an architecture with intrusion tolerance, called SITAR (Scalable Intrusion Tolerant Architecture) and described the stochastic behavior of the system by discrete-time semi-Markov process. They also derived the mean time length to security failure. Imaizumi, Kimura and Yasui [4] considered an intrusion tolerant system subject to DoS (Denial of Service) attacks (see *e.g.* [2]) and gave a continuous-time semi-Markov model. They formulated the long-run average cost and derived the optimal monitoring time of illegal access for minimizing it. Recently, VoIP (Voice over IP) network system [10] was modeled by the continuous-time Markov chains from the viewpoint of security design. In this way, several stochastic models have been developed with the aim of quantitative evaluation of information security.

In this paper we focus on the DoS attacks similar to Madan et al. [7], [8] and Imaizumi, Kimura and Yasui [4], and quantitatively evaluate the security of intrusion tolerant systems with preventive maintenance. In the DoS attacks, the attackers detect the vulnerabilities in server applications and make the network traffic increasing extremely by sending a large amount of illegal data. To protect the information assets from such malicious threats, the preventive maintenance would be useful for tolerating the security faults. The typical example of preventive maintenance is the patch management. If the vendors can know the vulnerable parts in the server applications in advance, they can release the patch before the malicious attackers detect them. In fact, the full vendors or the computer emergency response team/coordination center (CERT/CC) are always monitoring the system vulnerabilities reported by benign users or themselves, even after releasing the applications. More specifically, we develop two semi-Markov cost models and describe the stochastic behavior of two intrusion tolerant systems with different preventive maintenance policies. The optimal preventive maintenance schedules are analytically derived to minimize the long-run average costs. In numerical examples, we derive the optimal preventive maintenance policies

and their associated long-run average costs, and further perform the sensitivity analysis of the model parameters.

2 Model 1

2.1 Model Description

Figure 1 depicts the transition diagram of Model 1. Suppose that the server system starts operating at time $t = 0$ with *Normal State*; G . If attackers or hackers detect the vulnerability of a server application, the state makes a transition to *Vulnerable State*; V , where the transition time from G to V has the continuous cumulative distribution (c.d.f.) $F_0(t)$ with mean $\mu_0 (> 0)$. Once the malicious attack by an attacker begins, the system state changes to *Attack State*; A and the server operation stops for corrective maintenance, where the transition time from V to A is given by a random variable having the continuous c.d.f. $F_a(t)$ and mean $\mu_a (> 0)$. In this phase, if the minor corrective maintenance in a failure probable state is performed such as data recovery, the system can be recovered from the failure probable state to the normal one, and can become as good as new. The transition time from State A to State G is given by the generally distributed random variable with the c.d.f. $F_t(t)$ and mean $\mu_t (> 0)$. However, the system state may go to *System Failure State*; F before completing the minor corrective maintenance, where the transition time from A to F obeys the c.d.f. $F_f(t)$ with mean $\mu_f (> 0)$. Since this state is the system down state, the major recovery operation such as data initialization or system restart has to be carried out. The completion time to recover the server system from the system failure state is given by the non-negative continuous random variable with the c.d.f. $F_r(t)$ and mean $\mu_r (> 0)$.

On the other hand, if the vulnerable state V is detectable by vulnerability identifiers like a benign user, it may be effective to trigger the preventive maintenance before the vulnerabilities are detected by malicious attackers. As a plausible scenario on preventive maintenance, suppose that a benign user discovers the application vulnerability faster than the attackers, and discloses its information to the full vendor or the CERT/CC as well as his or her personal community. Then the patch management is an important issue for the vendor. When the development period of patch is relatively shorter, is the quick release of the patch really beneficial? If the vulnerable state is seldom detected, it would be better to release the patch from the vendor as soon as possible. However, if the similar vulnerable states may come repeatedly, the frequent release of patches may lead to the large overhead in operation. Define *Preventive Maintenance State*; M . If the preventive maintenance is triggered before the system becomes vulnerable, the system operation is stopped and the state goes to M from V . Without any loss of generality, define the transition time from V to A is distributed with the following c.d.f.:

$$F_m(t) = \begin{cases} 1 & (t \geq t_0) \\ 0 & (t < t_0). \end{cases} \quad (1)$$

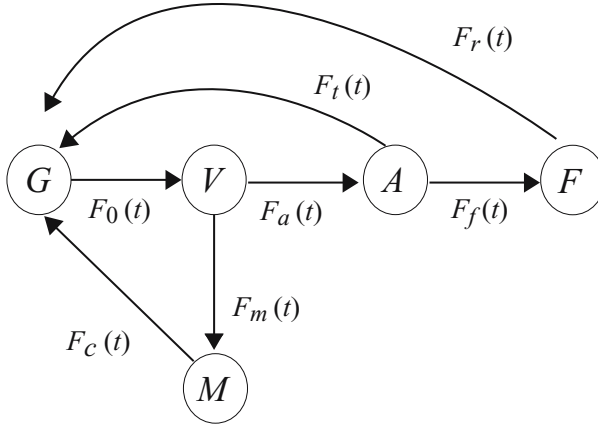


Fig. 1. Semi-Markov transition diagram of Model 1

This means that the preventive maintenance is performed at every t_0 time unit after the vulnerability is detected (this assumption is relaxed in the latter discussion). Once the preventive maintenance starts, it completes after the random time interval with the c.d.f. $F_c(t)$ and mean μ_c , so that the server system can be recovered similar to the state just before the vulnerability is detected. In the scenario of patch management, the time t_0 indicates a trigger to begin developing the patch. The same cycle repeats again and again over an infinite time horizon. Since the underlying stochastic process is a semi-Markov process, we can apply the standard technique to study it.

Define the one-step transition probability of Model 1 and its Laplace-Stieltjes transform (LST) by $Q_{ij}(t)$, $i, j \in \{G, V, A, F, M\}$, $i \neq j$ and $q_{ij}(s) = \int_0^\infty \exp\{-st\} dQ_{ij}(t)$, respectively. Then it is evident to obtain

$$q_{GV}(s) = \int_0^\infty \exp\{-st\} dF_0(t), \quad (2)$$

$$q_{VM}(s) = \int_0^\infty \exp\{-st\} \bar{F}_a(t) dF_m(t), \quad (3)$$

$$q_{VA}(s) = \int_0^\infty \exp\{-st\} \bar{F}_m(t) dF_a(t), \quad (4)$$

$$q_{AG}(s) = \int_0^\infty \exp\{-st\} \bar{F}_f(t) dF_t(t), \quad (5)$$

$$q_{AF}(s) = \int_0^\infty \exp\{-st\} \bar{F}_t(t) dF_f(t), \quad (6)$$

$$q_{FG}(s) = \int_0^\infty \exp\{-st\} dF_r(t), \quad (7)$$

$$q_{MG}(s) = \int_0^\infty \exp\{-st\} dF_c(t), \quad (8)$$

where in general $\bar{\psi}(\cdot) = 1 - \psi(\cdot)$.

Next we define the recurrent time distribution from State G to State G again by $H_{GG}(t)$. Then the LST of the recurrent time distribution is given by

$$\begin{aligned} h_{GG}(s) &= \int_0^{\infty} \exp\{-st\} dH_{GG}(t) \\ &= q_{GV}(s)q_{VA}(s)q_{AG}(s) + q_{GV}(s)q_{VA}(s)q_{AF}(s)q_{FG}(s) \\ &\quad + q_{GV}(s)q_{VM}(s)q_{MG}(s). \end{aligned} \quad (9)$$

Suppose that the system state is G at time $t = 0$ with probability one. We define the transition probability from G to $j \in \{G, V, A, F, M\}$ at an arbitrary time $t (> 0)$ and its LST by $P_{Gj}(t)$ and $p_{Gj} = \int_0^{\infty} \exp\{-st\} dP_{Gj}(t)$, respectively. Then, we have

$$p_{GG}(s) = \bar{q}_{GV}(s)/\bar{h}_{GG}(s), \quad (10)$$

$$p_{GV}(s) = q_{GV}(s) \left(\bar{q}_{VA}(s) - q_{VM}(s) \right) / \bar{h}_{GG}(s), \quad (11)$$

$$p_{GA}(s) = q_{GV}(s)q_{VA}(s) \left(\bar{q}_{AG}(s) - q_{AF}(s) \right) / \bar{h}_{GG}(s), \quad (12)$$

$$p_{GF}(s) = q_{GV}(s)q_{VA}(s)q_{AF}(s)\bar{q}_{FG}(s)/\bar{h}_{GG}(s), \quad (13)$$

$$p_{GM}(s) = q_{GV}(s)q_{VM}(s)\bar{q}_{MG}(s)/\bar{h}_{GG}(s). \quad (14)$$

It is not so easy to take the inversion of the above LSTs in Eqs. (10)–(14). Instead, by taking the limitation, we can derive the limiting transition probability $P_j = \lim_{t \rightarrow \infty} p_{G,j}(t)$, $j \in \{G, V, A, F, M\}$, *i.e.*,

$$P_G = \frac{\mu_0}{\mu_0 + \int_0^{t_0} \bar{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \bar{F}_a(t_0)}, \quad (15)$$

$$P_V = \frac{\int_0^{t_0} \bar{F}_a(t) dt}{\mu_0 + \int_0^{t_0} \bar{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \bar{F}_a(t_0)}, \quad (16)$$

$$P_A = \frac{\alpha F_a(t_0)}{\mu_0 + \int_0^{t_0} \bar{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \bar{F}_a(t_0)}, \quad (17)$$

$$P_F = \frac{\beta F_a(t_0)}{\mu_0 + \int_0^{t_0} \bar{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \bar{F}_a(t_0)}, \quad (18)$$

$$P_M = \frac{\mu_c \bar{F}_a(t_0)}{\mu_0 + \int_0^{t_0} \bar{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \bar{F}_a(t_0)}, \quad (19)$$

where

$$\alpha = \int_0^{\infty} t \bar{F}_t(t) dF_f(t) + \int_0^{\infty} t \bar{F}_f(t) dF_t(t), \quad (20)$$

$$\beta = \mu_r \int_0^{\infty} \bar{F}_t(t) dF_f(t). \quad (21)$$

In Eqs. (20) and (21), α and β imply the mean transition time from State A to the subsequent state and the mean transition time from State A to State G

through State F , respectively. From the results above, the semi-Markov model here is ergodic and the related stationary measures like the long-run average cost exist.

2.2 Optimal Preventive Maintenance Policy

Define the following cost parameters:

- $c_m (> 0)$: preventive maintenance cost per unit time
- $c_t (> 0)$: minor recovery cost per unit time
- $c_r (> 0)$: major recovery cost per unit time.

Then, the long-run average cost for the steady state in Model 1, $C_1(t_0)$, is formulated by

$$C_1(t_0) = \lim_{t \rightarrow \infty} \frac{E[\text{total cost during } (0, t)]}{t} = c_m P_M + c_t P_A + c_r P_F = U_{c1}(t_0)/T_1(t_0), \quad (22)$$

where

$$U_{c1}(t_0) = c_m \mu_c \overline{F}_a(t_0) + c_t \alpha F_a(t_0) + c_r \beta F_a(t_0), \quad (23)$$

$$T_1(t_0) = \mu_0 + \int_0^{t_0} \overline{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \overline{F}_a(t_0). \quad (24)$$

We make the following parametric assumptions:

- (A-1)** $c_m \mu_c < c_t \alpha + c_r \beta$,
- (A-2)** $\beta > \mu_c$.

Assumption **(A-1)** means that the sum of both mean recovery costs from the failure probable state and the system failure state is always greater than the mean preventive maintenance cost. Also, Assumption **(A-2)** implies that the mean time to recover the system after a system failure is always greater than the mean time required by the preventive maintenance. These two assumptions are needed to motivate the optimal preventive maintenance policy considered here. Then, we can characterize the optimal preventive maintenance policy minimizing the long-run average cost in Model 1 as follows.

Theorem 1. (1) Suppose that the c.d.f. $F_a(t)$ is strictly IFR (Increasing Failure Rate) under the assumptions **(A-1)** and **(A-2)**. Define the non-linear function:

$$q_{c1}(t_0) = (c_t \alpha + c_r \beta - c_m \mu_c) r_a(t_0) T_1(t_0) - \{1 + (\alpha + \beta - \mu_c) r_a(t_0)\} U_{c1}(t_0), \quad (25)$$

where $r_a(t) = (dF_a(t)/dt)/\overline{F}_a(t)$ is the failure rate.

- (i) If $q_{c1}(0) < 0$ and $q_{c1}(\infty) > 0$, then there exists a unique optimal preventive maintenance time t_0^* ($0 < t_0^* < \infty$) satisfying $q_{c1}(t_0^*) = 0$. The minimum long-run average cost is then given by

$$C_1(t_0^*) = \frac{(c_t\alpha + c_r\beta - c_m\mu_c)r_a(t_0^*)}{1 + (\alpha + \beta - \mu_c)r_a(t_0^*)}. \quad (26)$$

- (ii) If $q_{c1}(0) \geq 0$, then $t_0^* = 0$, *i.e.*, it is optimal to trigger the preventive maintenance just after the vulnerability is detected. Then the minimum long-run average cost is given by

$$C_1(t_0^*) = C_1(0) = \frac{c_m\mu_c}{\mu_0 + \mu_c}. \quad (27)$$

- (iii) If $q_{c1}(\infty) \leq 0$, then $t_0^* \rightarrow \infty$, *i.e.*, it is optimal not to perform the preventive maintenance even after the vulnerability is detected. Then the minimum long-run average cost is given by

$$C_1(t_0^*) = C_1(\infty) = \frac{c_t\alpha + c_r\beta}{\mu_0 + \mu_a + \alpha + \beta}. \quad (28)$$

(2) Suppose that the c.d.f. $F_a(t)$ is DFR (Decreasing Failure Rate) under the assumptions **(A-1)** and **(A-2)**. If $C_1(0) < C_1(\infty)$, then $t_0^* = 0$ otherwise $t_0^* \rightarrow \infty$.

Proof: Differentiating the function $C_1(t_0)$ with respect to t_0 and setting it equal to zero imply $q_{c1}(t_0) = 0$. Further differentiation of $q_{c1}(t_0)$ yields

$$\frac{q_{c1}(t_0)}{dt_0} = \frac{dr_a(t_0)}{dt} \left\{ (c_t\alpha + c_r\beta - c_m\mu_c)T_1(t_0) - (\alpha + \beta - \mu_c)U_{c1}(t_0) \right\}. \quad (29)$$

If $F_a(t)$ is strict IFR, from the assumptions **(A-1)** and **(A-2)**, it is obvious that the right-hand-side of Eq. (29) takes a positive value for an arbitrary t_0 and that the function $q_{c1}(t_0)$ is an increasing function of t_0 . From this, the long-run average cost $C_1(t_0)$ is a quasi-convex function of t_0 , so that if $q_{c1}(0) < 0$ and $q_{c1}(\infty) > 0$, then there exists a unique optimal solution t_0^* ($0 < t_0^* < \infty$) which satisfies $q_{c1}(t_0^*) = 0$. In the cases of $q_{c1}(0) \geq 0$ and $q_{c1}(\infty) \leq 0$, the long-run average cost $C_1(t_0)$ becomes increasing and decreasing in t_0 , and the optimal solution is given by $t_0^* = 0$ and $t_0^* \rightarrow \infty$, respectively. If $F_a(t)$ is DFR, the long-run average cost $C_1(t_0)$ is a quasi-concave function of t_0 , and the result is trivial.

3 Model 2

3.1 Model Description

In Model 1 it was assumed that the vulnerable state V could be detectable by the vulnerability identifiers and that the development of the patch could be

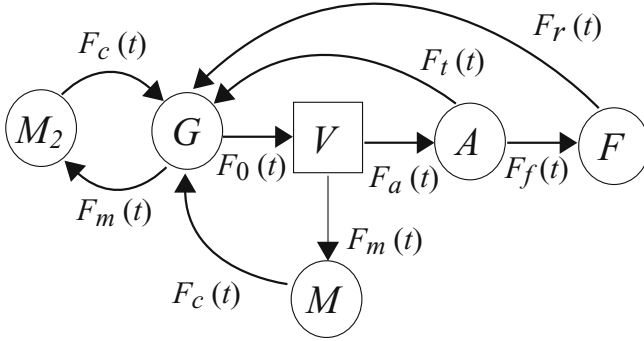


Fig. 2. MRGP transition diagram of Model 2

started after the time t_0 measured from the vulnerable state V elapsed. However, this assumption can not be always validated, because the vendor can not know the detection timing of vulnerabilities by malicious attackers. To resolve this problem, we consider another stochastic model referred as Model 2 in Fig. 2. That is, the preventive maintenance is triggered at the periodic time interval measured from State G . In Fig. 2, the circles and the square denote regeneration points and a non-regeneration point, respectively, so that the underlying stochastic process is reduced to a Markov regenerative process (MRGP) which belongs to the wider class than the semi-Markov processes.

However, as well known, the MRGP can be translated to the usual semi-Markov process by changing the definition of the underlying states. Figure 3 illustrates the translated semi-Markov transition diagram of the MRGP in Fig. 2, where we define two new states:

Normal State; G'

Preventive Maintenance State; M'

and the Stieltjes convolution operator by ‘ $*$ ’, i.e.,

$$F_0 * F_a(t) = \int_0^t F_0(t-x) dF_a(x). \tag{30}$$

Similar to the previous discussion, we define the one-step transition probability and its LST by $Q_{ij}(t)$, $i, j \in \{G', A, F, M'\}$, $i \neq j$ and $q_{ij}(s) = \int_0^\infty \exp\{-st\} dQ_{ij}(t)$, respectively. Then it is immediate to see that

$$q_{G'A}(s) = \int_0^\infty \exp\{-st\} \overline{F}_m(t) dG(t), \tag{31}$$

$$q_{AG'}(s) = \int_0^\infty \exp\{-st\} \overline{F}_f(t) dF_t(t), \tag{32}$$

$$q_{G'M'}(s) = \int_0^\infty \exp\{-st\} \overline{G}(t) dF_m(t), \tag{33}$$

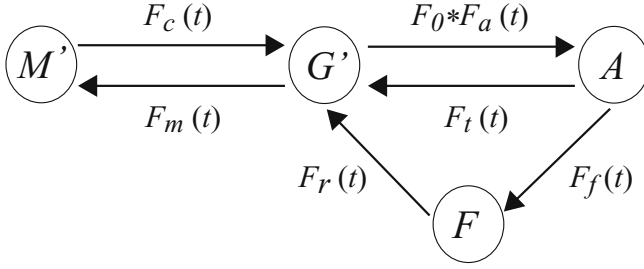


Fig. 3. Translated semi-Markov transition diagram of Model 2

$$q_{M'G'}(s) = \int_0^{\infty} \exp\{-st\} dF_c(t), \quad (34)$$

$$q_{AF}(s) = \int_0^{\infty} \exp\{-st\} \bar{F}_t(t) dF_f(t), \quad (35)$$

$$q_{FG'}(s) = \int_0^{\infty} \exp\{-st\} dF_r(t), \quad (36)$$

where $G(t) = F_0(t) * F_a(t)$.

For the recurrent time distribution from State G' to State G' again, $H_{G'G'}(t)$, we obtain the LST:

$$\begin{aligned} h_{G'G'}(s) &= \int_0^{\infty} \exp\{-st\} dH_{G'G'}(t) \\ &= q_{G'M'}(s)q_{M'G'}(s) + q_{G'A}(s)q_{AG'}(s) \\ &\quad + q_{G'A}(s)q_{AF}(s)q_{FG'}(s). \end{aligned} \quad (37)$$

Given the initial state G' at time $t = 0$, the LSTs of transition probabilities $P_{G'j}(t)$, $j \in \{G', A, F, M'\}$ at an arbitrary time $t (> 0)$ are given by

$$p_{G'G'}(s) = \left(\bar{q}_{G'A}(s) - q_{G'M'}(s) \right) / \bar{h}_{G'G'}(s), \quad (38)$$

$$p_{G'A}(s) = q_{G'A}(s) \left(\bar{q}_{AG'}(s) - q_{AF}(s) \right) / \bar{h}_{G'G'}(s), \quad (39)$$

$$p_{G'F}(s) = q_{G'A}(s) q_{AF}(s) \bar{q}_{FG'}(s) / \bar{h}_{G'G'}(s), \quad (40)$$

$$p_{G'M'}(s) = q_{G'M'}(s) \bar{q}_{M'G'}(s) / \bar{h}_{G'G'}(s). \quad (41)$$

In a fashion similar to Model 1, it can be seen that the limiting transition probabilities $P_j = \lim_{t \rightarrow \infty} p_{G',j}(t)$, $j \in \{G', A, F, M'\}$ are given by

$$P_{G'} = \frac{\int_0^{t_0} \bar{G}(t) dt}{\int_0^{t_0} \bar{G}(t) dt + \alpha G(t_0) + \beta G(t_0) + \mu_c \bar{G}(t_0)}, \quad (42)$$

$$P_A = \frac{\alpha G(t_0)}{\int_0^{t_0} \bar{G}(t) dt + \alpha G(t_0) + \beta G(t_0) + \mu_c \bar{G}(t_0)}, \quad (43)$$

$$P_F = \frac{\beta G(t_0)}{\int_0^{t_0} \overline{G}(t) dt + \alpha G(t_0) + \beta G(t_0) + \mu_c \overline{G}(t_0)}, \quad (44)$$

$$P_{M'} = \frac{\mu_c \overline{G}(t_0)}{\int_0^{t_0} \overline{G}(t) dt + \alpha G(t_0) + \beta G(t_0) + \mu_c \overline{G}(t_0)}. \quad (45)$$

3.2 Optimal Preventive Maintenance Policy

In Model 2, the long-run average cost $C_2(t_0)$ is formulated as

$$\begin{aligned} C_2(t_0) &= \lim_{t \rightarrow \infty} \frac{E[\text{total cost during } (0, t)]}{t} \\ &= c_m P_{M'} + c_t P_A + c_r P_F = U_{c2}(t_0)/T_2(t_0), \end{aligned} \quad (46)$$

where

$$U_{c2}(t_0) = c_m \mu_c \overline{G}(t_0) + c_t \alpha G(t_0) + c_r \beta G(t_0), \quad (47)$$

$$T_2(t_0) = \int_0^{t_0} \overline{G}(t) dt + \alpha G(t_0) + \beta G(t_0) + \mu_c \overline{G}(t_0). \quad (48)$$

We give the following result to characterize the optimal preventive maintenance policy for Model 2, without the proof.

Theorem 2. (1) Suppose that the c.d.f. $F_a(t)$ is strictly IFR under the assumptions **(A-1)** and **(A-2)**. Define the non-linear function:

$$\begin{aligned} q_{c2}(t_0) &= (c_t \alpha + c_r \beta - c_m \mu_c) r_{0a}(t_0) T_2(t_0) \\ &\quad - \{1 + (\alpha + \beta - \mu_c) r_{0a}(t_0)\} U_{c2}(t_0), \end{aligned} \quad (49)$$

where $r_{0a}(t) = (dG(t)/dt)/\overline{G}(t)$ is the failure rate.

(i) If $q_{c2}(0) < 0$ and $q_{c2}(\infty) > 0$, then there exists a unique optimal preventive maintenance time t_0^* ($0 < t_0^* < \infty$) satisfying $q_{c2}(t_0^*) = 0$. The minimum long-run average cost is then given by

$$C_2(t_0^*) = \frac{(c_t \alpha + c_r \beta - c_m \mu_c) r_{0a}(t_0^*)}{1 + (\alpha + \beta - \mu_c) r_{0a}(t_0^*)}. \quad (50)$$

(ii) If $q_{c1}(0) \geq 0$, then $t_0^* = 0$ and the minimum long-run average cost is given by

$$C_2(t_0^*) = C_2(0) = c_m. \quad (51)$$

(iii) If $q_{c2}(\infty) \leq 0$, then $t_0^* \rightarrow \infty$ and the minimum long-run average cost is given by

$$C_2(t_0^*) = C_2(\infty) = \frac{c_t \alpha + c_r \beta}{\mu_0 + \mu_a + \alpha + \beta}. \quad (52)$$

(2) Suppose that the c.d.f. $F_a(t)$ is DFR under the assumptions **(A-1)** and **(A-2)**. If $C_2(0) < C_2(\infty)$, then $t_0^* = 0$ otherwise $t_0^* \rightarrow \infty$.

In Section 2 and Section 3, we derived the optimal preventive policies for respective models with aperiodic and periodic preventive maintenance schedules, respectively. In the following section, we calculate numerically the optimal preventive schedules and their associated long-run average costs, and compare them

Table 1. Dependence of parameters (k, λ) on the long-run average cost

| (k, λ) | $t_0 \rightarrow \infty$ | Model 1 | | | Model 2 | | |
|----------------|--------------------------|---------|--------------|---------------|---------|--------------|---------------|
| | | t_0^* | $C_1(t_0^*)$ | reduction (%) | t_0^* | $C_2(t_0^*)$ | reduction (%) |
| (2,5) | 119.3280 | 0.0105 | 8.7717 | 92.6491 | 45.5572 | 49.6777 | 58.3689 |
| (2,10) | 113.3180 | 0.0421 | 8.7709 | 92.2600 | 48.2156 | 47.2078 | 58.3406 |
| (2,15) | 107.8850 | 0.0949 | 8.7695 | 91.8714 | 50.8743 | 44.9717 | 58.3151 |
| (3,5) | 116.2460 | 0.3344 | 8.7606 | 92.4637 | 53.1873 | 38.2400 | 67.1041 |
| (3,10) | 107.8850 | 0.9586 | 8.7397 | 91.8991 | 57.6474 | 35.4980 | 67.0964 |
| (3,15) | 100.6460 | 1.7782 | 8.7124 | 91.3435 | 62.1078 | 33.1228 | 67.0898 |
| (4,5) | 113.3180 | 1.2623 | 8.7245 | 92.3009 | 60.5449 | 31.6771 | 72.0459 |
| (4,10) | 102.9490 | 3.2492 | 8.6515 | 91.5963 | 67.0879 | 28.7700 | 72.0541 |
| (4,15) | 94.3177 | 5.6576 | 8.5651 | 90.9189 | 73.6312 | 26.3515 | 72.0609 |

quantitatively. Also, we perform the sensitivity analysis of model parameters and investigate the effect of preventive maintenance policy in the intrusion tolerant system.

4 Numerical Examples

Suppose that the c.d.f. $F_a(t)$ is given by the gamma distribution with shape parameter k (> 0) and scale parameter λ (> 0):

$$F_a(t) = t^{k-1} \frac{\exp\{-t/\lambda\}}{\Gamma(k)\lambda^k} \quad (53)$$

and that the other transition probabilities are given by the exponential distributions, where the other model parameters are assumed as $\mu_0 = 168C\mu_f = 4C\mu_c = 3C\mu_t = 5$, $c_r = 2500$, $c_m = 500$ and $c_t = 750$.

Table 1 presents the dependence of distribution parameters (k, λ) on the optimal preventive maintenance policies and their associated long-run average costs. From this result, it would be effective to perform the preventive maintenance based on the optimality criterion. Comparing the case without the preventive maintenance, the effect of 91%~92% (60%~70%) cost reduction in Model 1 (Model 2) was found in each parameter setting. On the other hand, when Model 1 is compared with Model 2, Model 1 could reduce the 75%~85% average cost more than Model 2. This is a natural conclusion because the vulnerable states are always detectable in Model 1 but not in Model 2. For instance, if the vendors or the CERT/CC could detect the vulnerabilities more quickly than the malicious attackers, they will be able to reduce the operation cost effectively.

References

1. Deswarte, Y., Blain, L., Fabre, J.C.: Intrusion tolerance in distributed computing systems. In: Proceedings of 1991 IEEE Symposium on Research in Security and Privacy, pp. 110–121. IEEE Press, Los Alamitos (1991)

2. Garber, L.: Denial-of-service attacks rip the Internet. *IEEE Computer* 33(4), 12–17 (2000)
3. Gupta, V., Lam, V., Ramasamy, H.V., Sanders, W.H., Singh, S.: Dependability and performance evaluation of intrusion-tolerant server architectures. In: de Lemos, R., Weber, T.S., Camargo Jr., J.B. (eds.) *LADC 2003*. LNCS, vol. 2847, pp. 81–101. Springer, Heidelberg (2003)
4. Imaizumi, M., Kimura, M., Yasui, K.: Reliability analysis of a network server system with illegal access. In: Yun, W.Y., Dohi, T. (eds.) *Advanced Reliability Modeling II*, pp. 40–47. World Scientific, Singapore (2006)
5. Jonsson, E., Olovsson, T.: A quantitative model of the security intrusion process based on attacker behavior. *IEEE Transactions on Software Engineering* 23(4), 235–245 (1997)
6. Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., Dobson, J., McDermid, J., Gollmann, D.: Towards operational measures of computer security. *Journal of Computer Security* 2(2/3), 211–229 (1993)
7. Madan, B.B., Goseva-Popstojanova, K., Vaidyanathan, K., Trivedi, K.S.: Modeling and quantification of security attributes of software systems. In: *DSN 2002*. Proceedings of International Conference on Dependable Systems and Networks, pp. 505–514. IEEE CS Press, Los Alamitos (2002)
8. Madan, B.B., Goseva-Popstojanova, K., Vaidyanathan, K., Trivedi, K.S.: A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance Evaluation* 56(1/4), 167–186 (2004)
9. Ortalo, R., Deswarte, Y., Kaaniche, M.: Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Transactions on Software Engineering* 25(5), 633–650 (1999)
10. Pant, H., McGee, A.R., Chandrashekar, U., Richman, S.H.: Optimal availability and security for IMS-based VoIP networks. *Bell Labs Technical Journal* 11(3), 211–223 (2006)
11. Singh, S., Cukier, M., Sanders, W.H.: Probabilistic validation of an intrusion tolerant replication system. In: *DSN 2003*. Proceedings of International Conference on Dependable Systems and Networks, pp. 615–624. IEEE CS Press, Los Alamitos (2003)
12. Stevens, F., Courtney, T., Singh, S., Agbaria, A., Meyer, J.F., Sanders, W.H., Pal, P.: Model-based validation of an intrusion-tolerant information system. In: *SRDS 2004*. Proceedings of 23rd IEEE Reliability Distributed Systems Symposium, pp. 184–194. IEEE CS Press, Los Alamitos (2004)
13. Stroud, R.: A qualitative analysis of the intrusion-tolerant capabilities of the MAF-TIA architecture. In: *DSN 2004*. Proceedings of International Conference on Dependable Systems and Networks, pp. 453–461. IEEE CS Press, Los Alamitos (2004)
14. Verissimo, P.E., Neves, N.F., Correia, M.: Intrusion-tolerant architectures: concepts and design. In: de Lemos, R., Gacek, C., Romanovsky, A. (eds.) *Architecting Dependable Systems*. LNCS, vol. 2677, pp. 3–36. Springer, Heidelberg (2003)
15. Verissimo, P.E., Neves, N.F., Cachin, C., Poritz, J., Powell, D., Deswarte, Y., Stroud, R., Welch, I.: Intrusion-tolerant middleware. *IEEE Security and Privacy* 4(4), 54–62 (2006)
16. Wang, H., Liu, P.: Modeling and evaluating the survivability of an intrusion tolerant database system. In: Gollmann, D., Meier, J., Sabelfeld, A. (eds.) *ESORICS 2006*. LNCS, vol. 4189, pp. 207–224. Springer, Heidelberg (2006)

An Efficient Mutual Authentication Scheme for EPCglobal Class-1 Generation-2 RFID System

N.W. Lo and Kuo-Hui Yeh

Department of Information Management
National Taiwan University of Science and Technology
No. 43, Sect. 4, Keelung Rd., Taipei, 106 Taiwan, R.O.C.
Fax number: 886-2-2737-6777
nwlo@cs.ntust.edu.tw,
D9409101@mail.ntust.edu.tw

Abstract. The nature of data security vulnerability and location privacy invasion of RFID systems have become a serious problem after hundreds of RFID application systems deployed all over the world. One of the promising solution directions is to provide an efficient authentication scheme with the compliance of international RFID standards such as EPCglobal, ISO18000-1 and ISO18000-6. In this study, we propose a novel authentication scheme for RFID systems with excellent data security properties, robust location privacy preservation and efficient data matching/retrieval mechanism. In addition, our scheme is compatible to EPCglobal Class-1 Generation-2 RFID standards because only simple cryptographic primitives such as pseudo-random number generator and cyclic redundancy check are required to be implemented in RFID tags.

Keywords: RFID, EPCglobal, Location Privacy, Data Security, Authentication, CRC.

1 Introduction

With extended information storage space, enhanced information retrieval capability removing the line of sight restriction, and new identification scheme which assigns every associated object with a unique code number, Radio Frequency Identification (RFID) systems have been pervasively deployed in our daily lives to replace optical bar code systems and make lots of innovating applications. Recent applications in manufacture industry, supply chain management, livestock tracking, and children/seniors location monitoring have demonstrated the potential benefits, impact, and success of RFID technology to human life in the near future.

A RFID system generally consists of radio frequency (RF) tags (i.e., transponders), RF readers (i.e., transceivers), and backend application server. Readers can broadcast an RF signal to inquiry tags of their contents without contacting them physically. Tags respond their resident data, typically including a unique serial number, to readers. RFID tags can be classified as two categories: active tag and passive tag. Active tags contain an on-board power source and can actively transmit data to the reader;

however, passive tags must be triggered by an RF signal through the forward channel from the reader and reply their contents via the backscatter channel. Because of active tags can push their reply signals further with their own power, active tags can be read by a reader from a longer distance than passive tags do.

In terms of logistics and retailer industry, the low-cost passive tags are far more charming than expensive active tags. The "Electronic Product Code"(EPC) standardized by the EPCglobal [3], a joint venture between EAN International (Europe) and UCC (USA), has become the dominant RFID technology standards on logistics. An EPC contains the manufacturer information, type of product, and a unique serial number to identify each individual item. Undoubtedly, the deployment of EPCs on all kinds of goods will invoke the greatest influence ever on the global world market. One of the most important standards proposed by the EPCglobal is the EPCglobal Class-1 Generation-2 RFID specification which defines the functionality and operation of a passive RFID tag. We abbreviate this type of RFID tag as GEN-2 RFID tag later in this paper. According to the EPC Class-1 GEN-2 standard [13], the major RFID features and restrictions are delineated as follows:

1. The operating energy of EPC passive tag is acquired from the RF signal generated by RFID interrogators (readers).
2. The wireless communication range of EPC passive tag is about 2 to 10 meters and EPC RFID systems operate within the frequency range of UHF band (800-960 MHz).
3. Because of the restriction on production cost, tag cannot provide sufficient computing resources to perform complex functions such as data/key encryption and hash function calculation.
4. A EPC Class-1 GEN-2 tag supports the following functions:
 - (a) 16-bit pseudo-random number generation (PRNG): a tag shall be able to generate 16-bits random or pseudo-random number Q using PRNG, have the ability to extract a subset of Q , and temporarily store at least two 16-bits random numbers.
 - (b) 16-bit cyclic redundancy code checksum: a tag shall implement the CRC function to protect and calibrate the commands/messages transmitted between tags and readers.
5. A 32-bits access PIN is used to trigger a tag into the secure mode, and then the tag is able to be read or written.
6. For the reason of privacy protection, a tag is permanently unusable when it receives a kill command with corresponding access PIN.
7. Tag memory shall be logically separated into four distinct sections:
 - (a) Reserved memory: 32-bit kill and access passwords are stored in this section.
 - (b) EPC memory: this part of memory contains 16-bit CRC, 16-bit protocol control (PC) and EPC with various sizes (64/96/256 bits).
 - (c) TID memory: this section stores ISO/IEC 15693 allocation class identifier (8-bits) and provides space for information of custom commands and optional features that a tag supports.
 - (d) User memory: this area is reserved for user-specific data.

In order to meet the low-cost manufacture requirement, GEN-2 RFID tag can only equip with very primitive computation power and functions. Since GEN-2 RFID tag

specification did not consider much regarding to user privacy and data security matters, many security attacks become the potential threats for the success of EPC-enabled RFID systems. For example, EPC-tagged objects in the supply chain make it easier for corporate espionage to remotely eavesdrop and gather unprotected information. A man can easily be traced where he went as long as an identified EPC tag (on an object item) is carried with him. Similarly, the monetary values of items a person worn or carried with him can be determined by an adversary effortlessly. Adversaries can also utilize the association rule on a set of EPC-tagged items to gain transaction information about items, and to track people without knowing their identities. Even more sophisticated security threats such as breadcrumb threat and RFID cloning [5] can potentially occur under current deployment. Hence, in order to survive from these potential security threats, a robust and secure RFID system should provide three important security and privacy functionalities: data content security during transmission, mutual authentication, and anonymity between communicating parties.

The vast literature devoted to RFID security field has been reviewed on several occasions [1, 2, 4-12]. However, some of them cannot be compatible with the EPC GEN-2 standards, and the others have weakness in terms of privacy protection or content security. Only few schemes [1, 2, and 6] can be implemented on EPC GEN-2 tags. Nevertheless, these schemes still suffer from threats such as replay attack, Denial-of-Service (DoS) attack, and identity tracking problem. In this paper, we first point out the security weaknesses of Chien and Chen's scheme [1] and derive a new mutual authentication scheme, which requires two authentication keys and two transaction data stored onto RFID tag memory associated with dedicated two-way message-passing authentication process. Based on security analysis, our scheme can resist security threats such as replay attack and DoS attack, and provide privacy protection such as anonymity and forward secrecy. Furthermore, the proposed scheme complies with the EPC GEN-2 standards and improves the efficiency of data retrieval at backend database.

The rest of this paper is organized as follows. Section 2 gives an introduction of EPC GEN-2 specifications and related RFID authentication research works. Next, we review Chien and Chen's scheme [1] and discuss their security weakness in Section 3. Section 4 presents a new authentication scheme to conquer these security pitfalls. The security analysis of our scheme is addressed in Section 5. Finally, we summarize our conclusion in Section 6.

2 Related Work

From information security point of view, the EPC GEN-2 standards do not thoroughly consider privacy invasion problems and data security issues. Only simple kill and access commands are specified in GEN-2 specifications to provide authentication function and data/privacy protection. In order to protect privacy-related information between communicating parties and to prevent counterfeit data attacks against RFID systems, many authentication schemes were introduced recently. Weis et al. [4] proposed two authentication mechanisms, hash-based access control and randomized access control, to achieve security and privacy aspects for RFID systems. In their schemes, a key in a RFID tag is either pre-defined or created by a pseudo-random number generator. In hash-based access control scheme, with the pre-defined shared

key as the argument, a tag's hash function generates its fixed tag identifier *metaID*. When a reader queries the tag, it replies with its *metaID*. In randomized access control scheme, the random-generated key R and hashed value of the pre-defined ID concatenated with key R are transmitted back to reader in response to reader's query. Since both schemes allow the reader to unlock the hash-locked tag by sending unencrypted pre-defined key or ID, an attacker can eavesdrop the communication channel and easily get all necessary information to either break these authentication schemes or trace specific tags. Based on the proposed brute-force ID search mechanism, the backend server can be overloaded easily by spending a lot of computation resources on ID matching for every query. More importantly, both authentication mechanisms cannot resist the replay attack and did not comply with EPC GEN-2 standards.

Ohkubo et al. [9] developed a mutual authentication scheme for RFID systems based on hashing chain mechanism. Their scheme aims to provide two security properties: indistinguishability and forward security. The indistinguishability of RFID tag indicates a tag's output must be indistinguishable from truly random values, while forward security denotes as even if the adversary acquires the secret data in a tag such as ID or access PIN, the attacker cannot trace the previous locations of the tag through revealed (eavesdropped) information in the past. However, this authentication mechanism cannot resist the replay attack either.

In [2] Henrici & Müller developed a novel scheme to prevent tag tracing problem by updating the identification of tag after each successful authentication. During the authentication process, the tag always responds a reader's query with the same hashed value before it updates its secret identification at the end of the query communications. This design allows an attacker to eavesdrop and trace a specific tag easily. In addition, the difference between the current transaction number and the last successful transaction number (ΔTID), which is used for a receiver(reader) to calculate the current transaction number (TID) stored in the tag, is broadcasted by the tag in a plain text format. Adversaries can utilize this ΔTID to invoke a replay attack.

Molnar and Wagner in [8] investigated the authentication process for book management systems in a library. Nonetheless, the PRF-based private authentication scheme proposed by Molnar et al. does not provide forward security to the tags stamped on books. Similarly, in [10] Rhee et al. used pseudo-random number generator and hash function to develop a challenge-response based RFID authentication protocol which does not offer forward security either.

An and Oh [12] proposed a new scheme, which is based on hash function and random-number generator function, to complete the authentication between the tag and the backend server. However, location tracking problem and replay attack are not resolved in their scheme. Yang et al. [11] pointed out the Henrici & Müller's scheme cannot solve location tracking problem and proposed a new scheme to solve this problem. Their scheme assumes the tag has the ability of performing PRNG function and hash function to generate different responses according to the random number sent from the reader. Unfortunately, Avoine et al. in [14] had pointed out the scheme proposed by Yang et al. cannot provide privacy to the tag carrier.

More recently, several new mechanisms [1, 6, 7], all compatible with the EPC GEN-2 specifications, have been proposed to achieve secure authentication process for RFID systems. Karthikeyan et al. [7] proposed a RFID authentication protocol based on XOR (exclusive OR) and matrix computation. Nevertheless, their scheme

cannot resist DoS attack, replay attack, and privacy-revealing problem. In [6] Duc et al. developed a simple authentication scheme by replying a server query with a random number R , $M_1 = CRC(EPC \| R) \oplus Key_i$, and $CRC(M_1 \oplus R)$. However, if attackers can intercept the "End Session" at the final communication step, the backend server will not update the old key in its database. Therefore, the opportunity for attackers to perform the DoS attack and counterfeit tag attack is open. Furthermore, this scheme is not able to provide forward secrecy either. Finally, Chien and Chen [1] improved the scheme invented by Karthikeyan et al. [7] and Duc et al. [6] to provide stronger privacy and security properties. However, their scheme still has space for improvement in terms of performance efficiency and data security. From the performance efficiency aspect, their scheme will generate heavy computation load on backend server because of the brute-force search mechanism applied for data match. In terms of data security, this scheme cannot resist the replay attack before both the tag and backend server complete their authentication process and key synchronization.

3 Security Analysis of Chien and Chen's Scheme

In this section, we briefly review Chien and Chen's authentication scheme, which was published in February 2007, in RFID systems and discuss the security weaknesses of their scheme.

Chien and Chen developed a mutual authentication, which is compatible with EPCglobal class 1 generation 2 standards. In their scheme, only lightweight operations, such as pseudo-random number generator (PRNG), XOR function, and CRC checksum function, are utilized for security enhancement and privacy preservation. Each tag, denoted as Tag_x , shares a unique identification EPC_x and the secret key values $K_{x,i}$ and $P_{x,i}$ with backend server, denoted as $Server$, during each authentication session i . In addition, $Server$ maintains two record of each shared secret key value (K_{new} , K_{old} , P_{new} , P_{old}) for each entry. This design is used to prevent their scheme against DoS attack. We illustrate the normal operation procedure of Chien and Chen's scheme as in Fig. 1.

1. $Reader_y \rightarrow Tag_x: N_1$

When $Reader_y$ sends a random number N_1 as a request to inquire Tag_x , Tag_x first generates a random number N_2 and computes the response value $M_1 = CRC(EPC_x \| N_1 \| N_2) \oplus K_{x,i}$

2. $Tag_x \rightarrow Reader_y \rightarrow Server: (M_1, N_1, N_2)$

Tag_x transmits (M_1, N_2) to $Reader_y$, which forwards (M_1, N_1, N_2) as an authentication request to $Server$. Once receiving the incoming authentication request, $Server$ iteratively retrieves key values (K_{new} , K_{old} , P_{new} , P_{old}) from each entry in backend database. Then, $Server$ computes the $I_{new} = M_1 \oplus K_{new}$ and $I_{old} = M_1 \oplus K_{old}$, and find the matching entry in backend database depending on which of the following conditional relationships holds: $I_{new} = CRC(EPC_x \| N_1 \| N_2) \oplus K_{x,i}$ or $I_{old} = CRC(EPC_x \| N_1 \| N_2) \oplus K_{x,i}$.

If $Server$ finds the matching entry, it computes $M_2 = CRC(EPC_x \| N_2) \oplus P_{new}$ or $M_2 = CRC(EPC_x \| N_2) \oplus P_{old}$ depending on which value (K_{new} or K_{old}) satisfies the previous verification process. Finally, $Server$ updates the shared symmetric key

value $P_{old}=P_{new}$, $K_{old}=K_{new}$, $K_{new}=PRNG(K_{new})$ and $P_{new}=PRNG(P_{new})$ through the PRNG function and sends $(M_2, ObjectData)$ to $Reader_y$.

3. Server \rightarrow Reader_y \rightarrow Tag_x: $(M_2, ObjectData)$

$Reader_y$ retrieves $ObjectData$ and forwards M_2 to Tag_x . Upon receiving M_2 , for the correctness of the incoming message, Tag_x verifies whether the $M_2 \oplus P_{x_i}$ and computed value $CRC(EPC_x || N_2)$ are identical or not. If both values are the same, Tag_x updates its shared symmetric key $K_{x_{i+1}}=PRNG(K_{x_i})$ and $P_{x_{i+1}}=PRNG(P_{x_i})$.

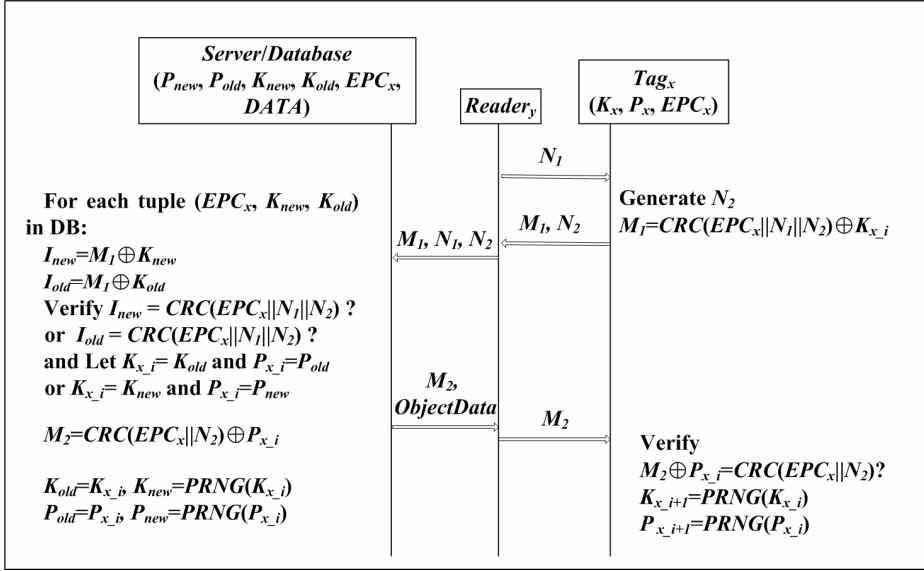


Fig. 1. Chien and Chen’s authentication scheme

After studying Chien and Chen’s authentication scheme, we have identified several weaknesses of their scheme. For the performance efficiency viewpoint, their scheme will generate heavy computation load on finding the matching data entry at backend server side due to *Server* have to XOR incoming message M_1 and the shared symmetric key (K_{new}, K_{old}) of each entry in backend database. For security aspect, before *Server* updates the shared symmetric key, attacker can easily perform replay attack to *Server* with iteratively issuing the eavesdropped legitimate authentication request (M_1, N_1, N_2) . In addition, the anonymity property also cannot be guaranteed in their scheme. We illustrate the attack scenario in Fig. 2. Before Tag_x updates the shared secret key, if the attacker sequentially sends two queries to Tag_x in a reasonable time, Tag_x will response two values M_1 and M_2 back to attacker. After XORing M_1 and M_2 , the shared secret key K_{x_i} will be eliminated. According to the known N_1, N_2, N_3 and N_4 , the attacker can easily trace the Tag_x without being noticed. For example, for the simplicity, we assume EPC_x, N_1, N_2, N_3 and N_4 are all 4-bits length. Attacker sequentially sends $N_1=0101$ and $N_3=0110$ as a request to Tag_x , and then Tag_x responds $M_1, M_2, N_2=1011$ and $N_4=1001$ to attacker. After computing the $M_1 \oplus M_2$ value, if the left

12-bits of computation result are (0000, 0011, 0010), attacker can identify Tag_x even if the EPC_x is unknown. Ex: $M_1 \oplus M_2 = CRC(EPC_x || N_1 || N_2) \oplus CRC(EPC_x || N_3 || N_4) = (EPC_x \oplus EPC_x, N_1 \oplus N_3, N_2 \oplus N_4, CRC_{M1} \oplus CRC_{M2}) = (0000, 0101 \oplus 0110, 1011 \oplus 1001, CRC_{M1} \oplus CRC_{M2}) = (0000, 0011, 0010, CRC_{M1} \oplus CRC_{M2})$.

Finally, their scheme cannot provide forward security either. We illustrate this weakness in Fig. 3. For each session, attacker first issues a query to Tag_x to get M_1 and sends M_1 to $Server$ for obtaining M_2 . Then, attacker stores these two values M_1 and M_2 without transmitting M_2 to Tag_x . Next, attacker eavesdrops the transmitted message M_3 and M_4 between Tag_x and other legitimate $Reader_y$. With these four transmitted M_1, M_2, M_3 and M_4 of each session, once Tag_x is compromised (the attacker would get the current secret information such as the EPC_x), the transmitted message M_3 and M_4 can be derived with known EPC_x, N_1, N_2, N_3 and N_4 . Hence, the forward security also cannot be guaranteed.

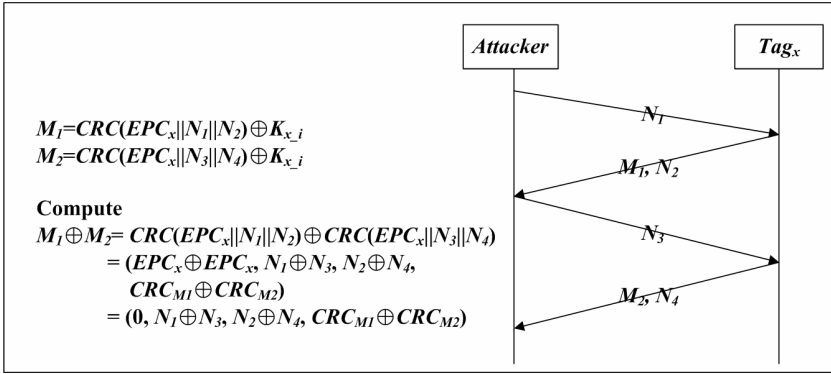


Fig. 2. Security weakness (anonymity) in Chien and Chen's scheme

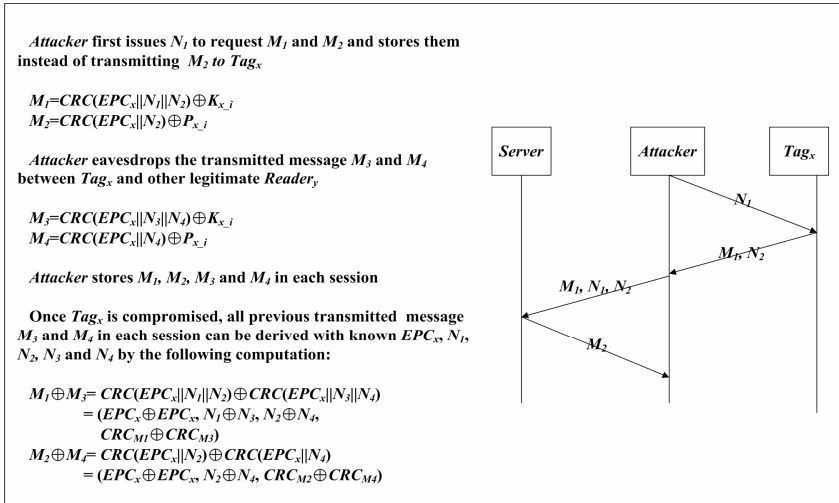


Fig. 3. Security weakness (forward security) in Chien and Chen's scheme

4 New Authentication Scheme

In this section we introduce a new derived mutual authentication scheme to achieve RFID system requirements for data security, privacy protection, and the efficiency of server utilization. Our scheme is designed to accommodate the EPC GEN-2 standard. The vulnerability of RFID tag is assumed. Once a tag was compromised, its contents can be retrieved and modified by the attacker. As previous proposed schemes, we assume that the attacker can monitor the communication channels and broadcast counterfeit messages between the RFID readers and tags, while the communication channels between the readers and the backend server are secure.

4.1 System Initialization

For each tag denoted as Tag_i , an initial setup is performed to store five various values in the tag's memory. The authentication key K_{x_0} and the database access key K_{DB} are generated from a PRNG function initially at the server side before inserting into Tag_i . These two keys (K_{x_0} and K_{DB}) are used to secure data. Note that the database access key K_{DB} will be shared by all tags within this database. A pre-defined value for the Electronic Product Code (EPC_x) and two default values for the transaction number (TID) and the last successful transaction number (LST) are assigned to both the server database and a corresponding tag during system initialization. For the sake of simplicity, the initial values of TID and LST are usually set to the same. In our scheme we have modified the Henrici & Müller's mechanism to prevent the replay attack. In addition, from the view point of forward security, the authentication key will be updated at both the querying server end and the responding tag end after each successful authentication. The authentication key after the i -th successful session update is denoted as K_{x_i} . For each EPC value, the backend server also maintains a record of twelve fields in the database including $EPC_{x_{new}}$ and $EPC_{x_{old}}$, the old and new authentication keys associated with this EPC_x (K_{old} and K_{new}), the shared database access key (K_{DB}), the old and new transaction numbers (TID_{old} and TID_{new}), the old and new values of last successful transaction numbers (LST_{old} and LST_{new}), the optional information ($DATA$), and the fast search key ($PRNG^m(EPC_{x_{new}})$ and $PRNG^m(EPC_{x_{old}})$). The fast search key is designed to find the corresponding data tuple in database efficiently during the reader query process, where m is a pre-defined positive integer and the dual-record design (*old* and *new*) is adopted to defense DoS attack. The initial values of the old and new authentication keys associated with EPC_x are both set to K_{x_0} . After system initialization, when the readers query RFID tags, the normal authentication process between reader and tag is activated as shown in Fig. 4. We describe the detail operation procedures in the next section.

4.2 Normal Authentication Operation

1. $Reader_y \rightarrow Tag_x$: Query

$Reader_y$ sends a *Query* signal as a challenge to the Tag_x .

2. $Tag_x \rightarrow Reader_y \rightarrow Server: M_1, M_2$

Tag_x first generates two random numbers n and N_1 where $n \leq m$, computes $TID = TID + 1$, $\Delta TID = TID - LST$, $M_1 = (CRC(EPC_x \| N_1 \| TID \| \Delta TID)) \oplus PRNG(K_{x_i} \oplus N_1)$ and $M_2 = CRC((PRNG^n(EPC_x) \| n \| N_1) \oplus K_{DB})$ sequentially, and sends the values (M_1, M_2) to the server. Note that when operating the XOR operation in our scheme, the size of each variant will be set to the same length by iteratively append the variant itself. For example, if the length of the $(CRC(EPC_x \| N_1 \| TID \| \Delta TID))$ and $PRNG(K_{x_i} \oplus N_1)$ are 144-bits and 16-bits individually, we first concatenate eight 16-bits $PRNG(K_{x_i} \oplus N_1)$ into one temporary 144-bits variant T and then XOR T with the $(CRC(EPC_x \| N_1 \| TID \| \Delta TID))$ as the output M_1 .

When the backend server receives the authentication request from $Reader_y$, it first use database access key K_{DB} to retrieve $PRNG^n(EPC_x)$, n and N_1 . Server then computes the $PRNG^m(EPC_x) = PRNG^{m-n}(PRNG^n(EPC_x))$, and finds the corresponding record entry from the database. After retrieving the values of related fields in the corresponding tuple, the server computes the values $H_1 = M_1 \oplus PRNG(K_{new} \oplus N_1)$ and $H_2 = M_1 \oplus PRNG(K_{old} \oplus N_1)$. Next, the binary string length function $LEN()$ and the binary string truncation function $TRUNC()$ are applied to calculate the following values:

$$\begin{aligned} I_{new} &= TRUNC(H_1, LEN(CRC(EPC_x \| N_1))), I_{old} = TRUNC(H_2, LEN(CRC(EPC_x \| N_1))), \\ TID_1 &= TRUNC(H_1, LEN(CRC(EPC_x \| N_1)), LEN(TID_{new})), \\ \Delta TID_1 &= TRUNC(H_1, LEN(CRC(EPC_x \| N_1)) + LEN(TID_{new}), LEN(TID_{new})) \\ TID_2 &= TRUNC(H_2, LEN(CRC(EPC_x \| N_1)), LEN(TID_{old})), \\ \Delta TID_2 &= TRUNC(H_2, LEN(CRC(EPC_x \| N_1)) + LEN(TID_{old}), LEN(TID_{old})) \end{aligned}$$

Note that the function $LEN(x)$ returns the length of binary string x , and the truncation function with two varieties $TRUNC(x, y)$ and $TRUNC(x, y, z)$ returns a partial binary string that contains either only the first y bits of the original string x or the substring with z bits of length started from the y -th bit position of the original string x , respectively.

Once the server has the intermediate values I_{new} , I_{old} , TID and ΔTID , the verification process is invoked to determine the authentication key hidden in the incoming tag response is the up-to-date one or the previous one. If $I_{new} = CRC(EPC_x \| N_1)$, then the authentication key from tag reply is up-to-date; the server computes $K_{x_i} = K_{new}$, $EPC_{x_i} = EPC_{new}$ and $TID^* = LST_{new} + \Delta TID_1$. Otherwise, the equation $I_{old} = CRC(EPC_x \| N_1)$ should be true, the equations $K_{x_i} = K_{old}$, $EPC_{x_i} = EPC_{old}$ and $TID^* = LST_{old} + \Delta TID_2$ are calculated by the server. Before generating the reply message to the reader, the server still needs to check abnormal conditions in order to prevent malicious attacks. Therefore, two logical relations, $TID^* \neq TID_1$ (or $TID^* \neq TID_2$) and $TID^* \leq TID_{old}$, are examined. If one of them was true, the server will discard the tag reply and deny further communication. The first logical relation, $TID^* \neq TID_1$ (or $TID^* \neq TID_2$), is adopted to detect counterfeit tag attack, while the second logical relation is to determine whether a replay attack is encountered.

Once the server successfully authenticates the tag in the previous step, it generates a random numbers N_2 and computes $M_3 = CRC(EPC_x \| N_2) \oplus PRNG(K_{x_i} \oplus N_2)$. At the same time the server will update the related fields of the corresponding EPC_x entry in

its database including the authentication keys, transaction numbers and the last successful transaction numbers. The update equations are listed in the sequence of execution order:

$$\begin{aligned} K_{old} &= K_{x_i}, K_{new} = PRNG(K_{x_i}), EPC_{x_{new}} = PRNG(EPC_{x_i} \oplus N_2), EPC_{x_{old}} = EPC_{x_i}, \\ TID_{new} &= LST_{new} = TID^*, TID_{old} = TID^*, LST_{old} = TID^* - \Delta TID, \\ PRNG^m(EPC_{x_{old}}) &= PRNG^m(EPC_x) \text{ and } PRNG^m(EPC_{x_{new}}) \end{aligned}$$

Afterwards, the server sends (M_3, N_2) with optional object data as a reply message to $Reader_y$.

3. Server \rightarrow Reader_y: $M_3, N_2, Object\ Data$

$Reader_y$ retrieves the product information (object data), if any, and forwards M_3 and N_2 to Tag_x .

4. Reader_y \rightarrow Tag_x: M_3, N_2

Upon receiving M_3 and N_2 , the tag verifies whether the equation $M_3 \oplus PRNG(K_{x_i} \oplus N_2) = CRC(EPC_x || N_2)$ holds or not. If the verification is passed, the tag will update its EPC code, authentication key and the last successful transaction number by applying the following equations: $K_{x_{i+1}} = PRNG(K_{x_i}), LST = TID, EPC_x = PRNG(EPC_x \oplus N_2)$.

5 Security Analysis

In this section, we analyze the proposed mutual authentication scheme and compare it with previous researches based on the following security and efficiency criterions.

Data security in RFID systems tends to focus on the data secrecy of messages transmitting between tags and readers. In our scheme data security is achieved by only transmitting bit-scrambled (XOR-ed) or transformed (PRNG-generated) data message such as M_1, M_2 , and M_3 . While N_2 is transmitted in plain text format, however, it is a random-generated one-time-valid number and must be associated with corresponding M_3 to perform meaningful computation. Even though these plain numbers can be modified or eavesdropped, the security robustness of meaningful data in transmitted messages will not be compromised. In addition, anonymity to both tags and readers can be provided in our scheme because only enciphered messages and one-time-valid random numbers are broadcasted during the reader-tag mutual communication periods of time. In other words, malicious attackers cannot easily trace a specific tag since there are no consistent clues revealed in each tag response. In the worst case, if a tag was compromised and all data stored in it was known by the adversary, the attacker still cannot trace back the trajectory of the compromised tag according to our authentication mechanism. Since the authentication key, EPC code and transaction numbers in a tag will be automatically updated after each successful authentication process, the forward security feature is naturally embedded in the proposed scheme.

Regarding to the tag privacy-revealing threat, the data matching mechanism of our scheme has a weakness; once a tag is compromised by an attacker, he can trace any targeted tag by utilizing the shared database access key K_{DB} until the targeted tag updates its EPC value. Consider the case that the attacker already knew the key K_{DB} .



Fig. 4. Proposed mutual authentication scheme

He can simply use a reader to query his target tags twice before those tags have chances to update their EPC values. Hence, for each tag the attacker gets two replied M_2 values i.e., $M_2 = CRC((PRNG^{n_1}(EPC_x) \parallel n_1 \parallel N_a) \oplus K_{DB})$ and $M_2' = CRC((PRNG^{n_2}(EPC_x) \parallel n_2 \parallel N_b) \oplus K_{DB})$, respectively. With the key K_{DB} the attacker can easily derive values of n_1 , n_2 , $PRNG^{n_1}(EPC_x)$ and $PRNG^{n_2}(EPC_x)$. By evaluating the equality relationship between $PRNG^u(EPC_x)$ and $PRNG^{u-v}(PRNG^v(EPC_x))$ where $u = Max(n_1, n_2)$ and $v = Min(n_1, n_2)$, the attacker can identify and trace a specific tag if it is included in the group of targeted tags. Even though there is a security weakness to our data matching scheme, we argue that once tags update their EPC values (EPC_x), the tags become anonymous again and it is not easy for an attacker to keep tracking the specific EPC-updated tag in a group of observed tags. In addition, the proposed matching mechanism can alleviate the computation burden in previous authentication schemes [1, 4, 6, 8-12].

In RFID systems, two of the easiest applicable attacks by malicious adversaries are replay attack and DoS attack. It is very hard, if not impossible, to prevent these kinds of security attacks in advance based on currently available security solutions. Therefore, after these attacks occurred, the resistance ability of a system becomes a very important measurement to its corresponding authentication scheme. In our scheme replay attack is defeated by acquiring the idea from Henrici and Müller in which the validity of a RFID tag message is associated with the transmitting transaction number (TID) and the difference (ΔTID) between the current TID and the last-stored TID in this tag. However, in our scheme we encipher the ΔTID as part of the tag message M_1 instead of sending ΔTID in a plain text format as Henrici et al. described in [2]. Consequently, it is more difficult for an adversary to figure out the value of ΔTID and perform replay attack accordingly. Regarding to DoS attack, our scheme maintains the current and the last updated pairs of authentication key, transaction number, and last successful transaction number, in terms of a EPC table entry. This design allows a tag with non-synchronized keys and transaction numbers due to DoS attack, can still be authenticated by the backend server and re-synchronize its data with the server database.

In terms of the efficiency of authentication process, how to reduce computation workload of the backend server during identity match process between a tag-replied identification and database entries is one of the important measurements to evaluate the practical implementation possibility of a RFID authentication mechanism. We adopt the concept of *Efficient Identity Scheme* in [15] and propose a special data retrieval mechanism. We utilize the m iterative computation result of PRNG function with EPC value as the starting seed (argument), to be the primary key of EPC entry table in the backend database. This design enables our scheme to spend less computation time and resources, and find a match record more quickly when a record match process is invoked by backend server, since the server only needs to calculate $m-n$ times of PRNG function iteratively with the received $PRNG^n(EPC_x)$ value as the starting seed before matching the computed result with the primary key of each EPC records. On the contrary, most of previous published schemes [1, 4, 6, 8-12] have to get each EPC entry, calculate its hashed value or perform other functional computation, then use the computed result to match with the received encrypted value from a RFID tag, and keep performing the same operation iteratively through all EPC records in the

database until a match is found. In addition, our scheme is compatible with EPC Class-1 GEN-2 standards because only pseudo-random number generator and basic XOR function are adopted and both functions are specified in EPC standards. The compliance of RFID standards of our authentication scheme greatly increases the possibility of its adoption by RFID systems vendors and corresponding industrial customers in practice.

Table 1 shows the comparison results among our scheme and the others in accordance with the security and efficiency requirements. Obviously, the proposed mutual authentication scheme is superior to the others by supporting all criterions.

Table 1. Comparison among proposed RFID authentication schemes

| | EPCglobal Class-1 Gen-2 standards compliance | Data security | Anonymity (resistance to tracking attack) | Resistance to replay attack | Resistance to DoS attack | Forward security | Backend server load |
|--|--|---------------|---|-----------------------------|--------------------------|------------------|---------------------|
| Weis et al. [4] (Hash-based access control) | X | X | X | X | O | X | O(1) |
| Weis et al. [4] (Randomized hash-locking access control) | X | X | O | X | O | X | O(k) |
| Ohkubo et al. [9] | X | O | O | X | O | O | O(k) |
| Henrici & Müller. [2] | X | O | X | O | O | X | O(1) |
| Rhee et al. [10] | X | O | O | X | O | X | O(k) |
| Molnar-Wagner [8] | X | O | O | X | O | X | O(k) |
| Yang et al. [11] | X | O | X | X | O | X | O(k) |
| An & Oh [12] | X | O | O | X | O | X | O(k) |
| Karthikeyan-Nesterenko [7] | O | O | X | X | X | X | O(1) |
| Duc et al. [6] | O | O | X | X | X | X | O(k) |
| Chien & Chen [1] | O | O | X | X | O | X | O(k) |
| Our scheme | O | O | O | O | O | O | O(m-n) |

k: the number of tuples in database
 m: server pre-defined value
 n: random number generated at each session where $m > n$

6 Conclusion

In this paper we present a new mutual authentication scheme for RFID systems. Our scheme makes the RFID authentication process more robust and secure by introducing dynamical mechanism to change the authentication key and the access key with different random numbers at each authentication phase. Furthermore, the scheme also reduces the workload of the backend server from iteratively retrieving and computing each tuple linearly in database. Finally, our scheme improves data security and privacy protection for RFID systems from the previous authentication schemes and is compatible with the EPC Class-1 GEN-2 standards. In brief, our scheme can defend against the serious replay attack and DoS attack. At the same time the scheme provides excellent privacy protection such as anonymity and forward secrecy.

Acknowledgments. The authors gratefully acknowledge the support from TWISC projects sponsored by the National Science Council, Taiwan, under the Grants No NSC 96-2219-E-001-001 and NSC 96-2219-E-011-008.

References

1. Chien, H.-Y., Chen, C.-H.: Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards. *Computer Standards & Interfaces* 29(2), 254–259 (2007)
2. Henrici, D., Müller, P.: Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. In: *PerSec 2004. Workshop on Pervasive Computing and Communications Security at IEEE PerCom 2004, Orlando, Florida, USA PERCOMW (March 14-17, 2004)*
3. EPCglobal, <http://www.EPCglobalinc.org/>
4. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: *Security in Pervasive Computing*, pp. 201–212 (2003)
5. Garfinkel, S.L., Juels, A., Pappu, R.: RFID Privacy: An overview of Problems and Proposed Solutions. *IEEE Security & Privacy Magazine* 3(3), 34–43 (2005)
6. Duc, D.N., Park, J., Lee, H., Kim, K.: Enhancing Security of EPCglobal GEN-2 RFID Tag against Traceability and Cloning. In: *The 2006 Symposium on Cryptography and Information Security, Hiroshima, Japan (January 17-20, 2006)*
7. Karthikeyan, S., Nesterenko, M.: RFID Security without Extensive Cryptography. In: *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 63–67 (2005)
8. Molnar, D., Wagner, D.: Privacy and Security in Library RFID: Issues, Practices, and Architectures. In: *CCS 2004. Conference on Computer and Communications Security*, pp. 210–219 (2004)
9. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic Approach to Privacyfriendly Tags. In: *RFID Privacy Workshop, MIT, MA (2003)*
10. Rhee, K., Kwak, J., Kim, S., Won, D.: Challenge-response Based RFID Authentication Protocol for Distributed Database Environment. In: Hutter, D., Ullmann, M. (eds.) *SPC 2005. LNCS, vol. 3450*, pp. 70–84. Springer, Heidelberg (2005)
11. Yang, J., Park, J., Lee, H., Ren, K., Kim, K.: Mutual Authentication Protocol for Low-cost RFID. In: *The Encrypt Workshop on RFID and Lightweight Crypto (2005)*
12. An, Y., Oh, S.: RFID System for User's Privacy Protection. In: *Asia-Pacific Conference on Communications*, pp. 516–519 (2005)
13. Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.0.9, <http://epcis.mit.edu/CS/files/folders/epcglobal/entry21.aspx>
14. Avoine, G., Dysli, E., Oechslin, P.: Reducing Time Complexity in RFID Systems. In: Preneel, B., Tavares, S. (eds.) *SAC 2005. LNCS, vol. 3897*, pp. 11–12. Springer, Heidelberg (2006)
15. Lo, N.W., Yeh, K.-H.: Novel RFID Authentication Schemes for Security Enhancement and System Efficiency. In: *SDM 2007. The 4th VLDB workshop on Secure Data Management, September. LNCS, Springer, Heidelberg (to appear, 2007)*

UPS – An Ubiquitous Proximity eService for Trust Collaboration

Yuan-Chu Hwang¹ and Soe-Tsyr Yuan²

¹ Department of Information Management, National United University, Taiwan
No. 1, Lien Da, Kung-Ching Li, Miao-Li 360, Taiwan, R.O.C.
yuanchu.hwang@gmail.com

² Department of Management Information Systems, National Chengchi University, Taiwan
No. 64, Sec. 2, ZhiNan Rd., Wenshan District, Taipei City 11605, Taiwan, R.O.C.
yuans@mis.nccu.edu.tw

Abstract. Ubiquitous e-service is one of the most recent links in the chain of evolution that has characterized the different eras of the internetworking environment. The ubiquitous proximity e-service highlights the collective effort focused on collecting the user group's power as the reference for ubiquitous trust decisions. In this paper, we define the ubiquitous proximity e-service and discuss the significance of ubiquitous proximity e-service. Simulation outcomes for trust decision quality enhancement show significant improvement in all kinds of environment settings. The ubiquitous proximity e-service makes it possible for users to collaborate with the nearby user groups for establishing a reliable and trustworthy interaction environment. It also facilitates and empowers the potential benefits of various ubiquitous e-service applications.

1 Changes of Proximity in the U-Commerce Era

The ongoing developments of ubiquitous commerce have brought human life into a new era. Classic social science studies long ago demonstrated that proximity frequently increases the rate of individuals communicating and affiliating in organizations and communities [1,4]. Proximity also develops strong norms of solidarity and cooperation. While advanced telecommunication technologies have led some to conclude that the problem of distance has been overcome, others argue that proximity remains essential to group functioning and that new technologies cannot eliminate the challenges faced by members of geographically-dispersed teams. The essentiality of proximity may be controversial, but the definition of proximity might change owing to technological innovations in the U-Commerce era.

We proposed Ubiquitous Proximity e-Service (UPS) for exploring collective wisdom in the ubiquitous environment. The UPS highlights the collective effort focused on collecting the user group's power as the reference for ubiquitous trust decisions. Some security design was elaborated in Hwang and Yuan [10], including three conceptual methodology designs: the privacy design, reputation management design, and trust management design. But in this paper, we focus on the theoretical support of proximity value.

The ubiquitous proximity e-service can be treated as a new scope of ubiquitous e-services that highlight the collective effort of proximity participants within a ubiquitous environment. Due to the dynamicity and complexity present in the ubiquitous world, it is unrealistic to expect humans to be able to reason and act effectively to address potential risks in the ubiquitous environment. In order to propose a new e-service paradigm that aims to mitigate potential risks and threats present in the ubiquitous e-service environment due to its flexible, dynamic, and collaborative nature, we will begin our discussion by considering the collaboration with proximal participants.

Sociologists and anthropologists have long recognized that people can feel close to distant others and develop common identities with distant others who they rarely or never meet. [2, 9] Besides geographical distance, in the U-Commerce era, proximity places increased emphasis on individual homophily personal characteristics. The principle of homophily provides the basis for numerous social interaction processes. The basic idea is simple: "people like to associate with similar others." [3, 11, 13] As mentioned above, ubiquitous proximity e-service stresses the collective efforts of participants in the dynamic environment. Homophylic user groups are more likely to combine the strength of different individuals to achieve specific objectives.

Furthermore, as stated in Metcalfe's Law: "the usefulness, or utility, of a network equals the square of the number of users." This law has been modified to consider the number and value of the network resources (i.e. available services). The Network Effect results from Metcalfe's Law, which states that, "Network effects refer to the notion that as more individuals participate in a network, the value of the network to each individual participant increases". Network adoption rate increases in proportion to network utility. Services become more valuable as more people use it, thus encouraging growing numbers of adopters.

Ubiquitous proximity e-service exploits the network effect and tries to enhance collective effort by gathering energy within a dynamic environment. The relationships within the ad-hoc ubiquitous environment involve social network theory. Interpersonal social relationships can be defined by tie strength as weak or strong ties based on the following combinations: time, emotional intensity, intimacy, and the reciprocal services which characterize the tie. [7]. According to Marsden and Campbell, tie strength depends on the quantity, quality, and frequency of knowledge exchange between actors, and can vary from weak to strong. Stronger ties are characterized by increased communication frequency and deeper, more intimate connections.

Although strong ties tend to provide greater social support than weak ties (emotional aid, goods and services, companionship, and a sense of belonging), weak ties tend to link individuals to other social worlds, providing new sources of information and other resources.[8] Their very weakness means that they tend to connect people who are more socially dissimilar than those connected via strong ties. Individuals with few weak ties within a community become isolated from receiving new information from outside circles and can only hear information re-circulated within their own clique of close friends [8]. A weak tie link linking strongly tied groups is termed a local bridge [7]. Weak ties contribute to social solidarity; community cohesion increases with the number of local bridges in a community [7].

According to Friedkin [5] the mix of weak and strong ties increases the probability of information exchange.

The ubiquitous e-service environments are in an ad-hoc composition where social relationships may not well spread. Strong ties may only rarely be available within this ad-hoc environment. The nature of ad-hoc e-service is such that rare connections between individuals are more likely to establish. Proximity may be the reason for participants establishing ties. Even weakness ties then have an opportunity to become strengthened interpersonal relationships.

Homophily (namely, love of the same) describes the tendency of individuals to associate and bond with similar others. Homophily has been found in numerous network studies. By highlighting the homophily of e-service participants, these isolated individuals can be treated as a group with proximity (that is: common goals, similar interests, etc.). Interpersonal ties can be established in addition to some interactions. Loose-coupled e-service participants thus can be empowered to form groups/clusters with weak ties. Proximity thus enables ad-hoc e-service participants to contribute their strength for ubiquitous collective wisdom.

2 Significance of Ubiquitous Proximity e-Service

The main value of ubiquitous proximity e-service utilizes the network effect from the collective effort of interpersonal social network. By obtaining unique, non-reproducible interpersonal experiences from e-service environments, those information sources originate and shape collective wisdom. The involvement of more participants further increases the possibility of strengthening collective wisdom. The collective value derives from individual mental proximity. The characteristics of proximity encourage loose-coupled or isolated individuals to form groups with weak tie relationships and facilitate the creation of collective wisdom. Information diffusion and gathering via the Peer-to-Peer method can obtain “unique” data sources. The following paragraphs discuss collective wisdom based on the proximity e-service environment and a critical trust issue regarding how to collaborate with unfamiliar strangers.

Collective wisdom has a similar meaning to the term “collective intelligence”, which describes intelligence based on the collaboration and competition of numerous individuals (an intelligence that appears to have a mind of its own). One pioneer of research on collective intelligence, George Pór, defined collective intelligence as: "the capacity of a human community to evolve toward higher order complexity thought, problem-solving and integration through collaboration and innovation." [6]

The collective wisdom regarding ubiquitous proximity e-service is based on social networks. Since ubiquitous proximity e-services may utilize Internet environments, they transmit information various ways: (1) the external method that permits effective information spread and diffusion; (2) the internal method that helps individuals to gather and obtain useful information via personal social networks. Proximity e-service participants propagate information voluntarily via their own social networks voluntarily. Information diffusion for proximity e-services is more efficient than in Internet environments, and weak ties help information propagation and diffusion via the personal networks and relationships of nearby users.

However, a critical problem exists regarding trust decisions for strangers, “Why individuals should share information with strangers in an unfamiliar environment?” This problem involves problems of both interpersonal trust and efficiency. Relying solely on fixed Internet it is impossible to establish such extensive interpersonal trust networks in an ad-hoc e-service environment. In the ad-hoc e-service environment, it is necessary to integrate social networks with trust issues. It can be said that ubiquitous e-service participants may also be unfamiliar with each other. However, in the real world, it is usually accepted that “trust” or “confidence” is necessary for commerce activities. Despite the need for precautions, it is said that: “you have to trust your partner”. The commerce environment is rife with asymmetric information, moral hazard, opportunism, and so on. Vulnerability exists in commerce environments. Nevertheless, collaboration may be necessary in many situations in which goals cannot be achieved by single units (persons, firms, groups etc.). Thus, ad-hoc e-service participants have to accept, at least, a minimum vulnerability to achieve cooperation with partners. An optimistic concept may increase the chance of collaboration becoming a reality. However, cautious assessments of interaction events are also crucial.

It is difficult for users to collaborate with complete strangers. No collective wisdom can be established in environments in which participants are completely isolated. A significant value of the proximity e-service lies in the increased possibility of establishing innovative social network relationships. From the interpersonal perspective, unfamiliar strangers can make connections with individuals who are proximal and homoplastic to him (that is, shared interests cause users to gather at a single exhibition). The strength of proximity gives people better chances to make interpersonal connections, including both weak ties (i.e. someone you know each other) and strong ties (i.e. good friends).

Similarity breeds connections. [12] Ubiquitous proximity e-service utilizes homophily to connect separated individuals via weak tie relationships. These weak connected groups together with their original owned interpersonal connections then can enhance the collective effort by extensive information sharing and cooperation. By combining those interpersonal tie relationships proximity e-services can more easily cause information diffusion and effectively encourage collective wisdom.

3 Justification of Theoretical Support

The concept of the small-world phenomenon was observed over 30 years ago in social systems. The small world phenomenon (also known as the small world effect) is the hypothesis that everyone in the world can be reached via a short chain of mutual acquaintances. Small-world behavior can be defined generally and physically by considering the efficiency of information exchange over the network. The proximity value benefits from the small world phenomenon, which gathers available information sources and facilitates collaboration within the ubiquitous e-service environment. There are two aspects of the justification of theoretical support for proximity value: **Efficiency** and **Cost**.

Since we have redefined the proximity in ubiquitous e-service environment. We will compare the value of ubiquitous proximity e-service with the Internet e-service environment. Comparisons are made between two scenarios: ZigBee-based ubiquitous proximity e-service environment and Internet-based WiMax e-service environment.

First, this study compares the chance to establish weak-tie connectivity for collective wisdom. Ubiquitous proximity e-service focuses on the characteristic of “Homophily”. As mentioned above: (1) People like to associate with similar others, (2) Similarity begets friendship, (3) People love those who are like themselves. Proximity e-service in ubiquitous environment is characterized by “geographical proximity” as well as “user characteristic proximity”. Homophily leads unfamiliar participants to form new connections. Participants may have the opportunity to make connections via weak-tie relationships, and may even have the opportunity to form interest groups. ZigBee supports the local range connections and thus is suitable for proximity e-service, which also emphasis on interacting with nearby participants. Compared to individuals who only have the “user characteristics” homophily, ubiquitous proximity e-service based on ZigBee has more opportunities for unfamiliar individuals to build some new relationships. (Since proximity e-service own both user characteristics homophily and geographic homophily). Proximity increases the opportunities for unfamiliar ubiquitous e-service participants to form weak-tie interpersonal relationships.

Internet-based WiMax makes it more convenient for mobile users to connect to the world. Although users may have the characteristic proximity in the internet-based WiMax environment, their geographic distances are significantly larger than in the ZigBee-based environment. (9.6 kilometers for WiMax versus 100 meter for ZigBee) Extensive service range is not the advantages for real-time interactions particularly given that e-service focuses on communicating with nearby participants. Since individuals may sometimes wish to make connection with other distant individuals. It is unrealistic to establish real-time interactions over long distances. According to Hill and Dunbar [15], social networks have a cap of approximately 150 individuals (above this size they cease to be effective). Increasing connection numbers by extending service range cannot improve social network efficiency. Furthermore, the homophily characteristics of broad range peer groups are looser than the surrounding proximal users in terms of network density. It is less efficient for individuals to perform real-time interactions or obtain e-services from service providers. The effect that weak-tie gathered from user characteristics homophily also exists in the internet-based WiMax environment. However, in the absence of geographical homophily, WiMax is weaker than the proximal range of ZigBee-based ubiquitous proximity e-service. In terms of the intensity of real-time interactions, ZigBee-based ubiquitous proximity e-service is stronger than Internet-based e-services.

Hereby, we have the first explanation for proximity e-service in ubiquitous environment as follows: **“Ubiquitous proximity e-service has better opportunities to build up weak-tie connectivity than internet e-service environment.”**

$$\rho_{\text{proximity}} > \rho_{\text{Internet}} \quad (1)$$

where ρ represents the probability of establishing interpersonal connections.

Second, this study compares the cost of establishing social relationships. The cost of establishing the social network can be various, including communications costs, the involvement of the social network, etc. All of these costs are related to communications between mobile devices. Transmissions increase with involvement of virtual sociality. However, increased communications generally result in increased power consumption for transmitting messages via mobile networks. Without loss of generality, this investigation uses power consumption as the communication cost which represents the cost of building interpersonal relationships. Indeed, mobile devices suffer power supply constraints. Without power supply, mobile users are isolated from their networks and their mobile device becomes useless. As mentioned above, ZigBee describes a standardized wireless protocol for personal area networking, or “WPAN”. ZigBee differs from other wireless standards in being designed to serve a diverse market of applications requiring low cost and low power wireless connectivity, and provides greater sophistication than was previously available for the price. ZigBee focuses on low data rate and low duty cycle connectivity, a segment that existing standards do not service well. WiMax supports wide range communications, but has higher power consumption than ZigBee, and thus requires higher capacity battery. According to Texas Instruments (TI), WiMax currently stays in the stage for mobile users accessing the broadband network. The mobility of WiMax will confront with roaming problem, power consumption problems, network switching issues, etc. in the future. Attempts to apply WiMax to mobile applications will meet these problems.

This study provides another explanation for proximity e-service in ubiquitous environments, as follows: **“ZigBee-based proximity e-service can establish social relationships more cheaply than Internet e-service environments.”**

$$\gamma_{\text{proximity}} < \gamma_{\text{Internet}} \quad (2)$$

γ represents the establishment cost for establishing interpersonal connections.

Information diffusion via proximity e-service environment. Unlike the fixed internet-based network topology, mobile ad hoc networks (MANETs) comprise mobile devices fitted with short range radio transmission. Devices can communicate within their respective radio ranges. The mobility of ubiquitous e-service participants leads to frequent topology changes in ubiquitous proximity e-service environment. Considering information diffusion efficiency within ubiquitous proximity e-service environments, this study found that traditional information propagation theory may not be applicable to current ubiquitous e-service environments. Ubiquitous proximity e-service benefits from social network theory and improves the diffusion efficiency through various tie relationships.

Based on the definition of economic small world, the economic small world focuses on the low cost and high efficiency of information propagation. Consider the information propagation between two nodes i and j . The path length (that is, distance) between the two nodes is defined as $\{d_{ij}\}$. Moreover, the information diffusion Efficiency(ϵ) is defined as $1/\{d_{ij}\}$. When distance $\{d_{ij}\} = +\infty$, Efficiency(ϵ)=0.

Ubiquitous proximity e-service is based on mobile ad-hoc network structure, in which users are generally unfamiliar with surrounding participant peers. In the absence of any existing relationships, those total strangers may not establish

connections. If $Peer_i$ and $Peer_j$ are totally unfamiliar with each other then no relationships exist between the two peers. Since the peers are unconnected, the path length (i) to (j) is $+\infty$, meaning $\{d_{ij}\} = +\infty$. Based on the efficiency definition, the Information Diffusion Efficiency is zero. ($\varepsilon=0$)

Two of the ideas mentioned above are: (1) Ubiquitous proximity e-service has a better chance of improving weak-tie connectivity than Internet e-service environment. (2) ZigBee-based ubiquitous proximity e-service has lower cost for establishing social relationships than Internet e-service environment.

Ad-hoc e-service environment's nature (i.e. short term lived identities) may cause participant unfamiliarity. In such e-service environment, proximity e-service has a better chance of establishing weak-tie connections with nearby peers while achieving lower communication costs.

Because ε is directly proportional to ρ . Additionally, ε is inversely proportional to γ . Accordingly, it was found that $\varepsilon = \beta (\rho/\gamma)$. Efficiency(ε) increases with increasing ρ . Higher Cost(γ) also leads to lower Efficiency(ε). In this formula, β is a constant greater than 1.

From (1) and (2), since $\rho_{\text{proximity}} > \rho_{\text{Internet}}$ and $\gamma_{\text{proximity}} < \gamma_{\text{Internet}}$, it is concluded that $\varepsilon_{\text{proximity}} > \varepsilon_{\text{Internet}}$

$$\varepsilon_{\text{proximity}} > \varepsilon_{\text{Internet}} \quad (3)$$

Some possible future scenarios are considered below:

(a) The service range of the Internet-based WiMax e-service environment is reduced, reducing in a situation where $\rho_{\text{proximity}} \geq \rho_{\text{Internet}}$. Since $\gamma_{\text{proximity}} < \gamma_{\text{Internet}}$, in which case the information diffusion efficiency of ubiquitous proximity e-service remains higher than in the Internet-based WiMax environment.

(b) Advanced technologies reduce communication costs, leading to $\gamma_{\text{proximity}} \cong \gamma_{\text{Internet}}$. Since $\rho_{\text{proximity}} < \rho_{\text{Internet}}$, in which case the information diffusion efficiency of ubiquitous proximity e-service remains higher than in the internet-based WiMax environment.

Neither of these situations influences the result. This study thus reaches the following conclusion: The Information Diffusion Efficiency in the ubiquitous proximity e-service environment exceeds that in the Internet-based environment.

4 Value of Proximity: A Case Scenario

Participant social relationships of a conference scenario resemble a small world network. Small world networks have shorter average path length between nodes and higher node clustering than in the case for a random distribution. Watts and Strogatz [14] demonstrate how social networks, electricity power grids and neural networks small world properties and how their model can be used to create graphs with such properties. The conference attendees inhabit a proximity e-service environment, which participants are in some level similarity of their interests in geographic proximity as well as cognitive proximity. Figure1 represents the conference proximity e-service scenario.

This study considers the following scenario that offers proximity e-service in a conference. The scenario involves a conference with numerous delegates, at which several sessions generally occur simultaneously. Attendees moving freely between sessions, depending on the subject and their interests. Relationships between colleagues and friends are considered strong-tie relationships. Meanwhile, familiar strangers describe individuals who are regularly encountered but with whom there are no interactions. Some strangers encountered repeatedly at the same conferences over consecutive days may be treated as familiar stranger during a later meeting in a restaurant. Familiar strangers can have different varieties of proximity to a given individual, with geographic proximity and cognitive proximity (interest in similar research topics) representing the possibility for strangers to form weak relationships with others.

Proximity implies lower communication cost and higher opportunity to establish weak-tie connections

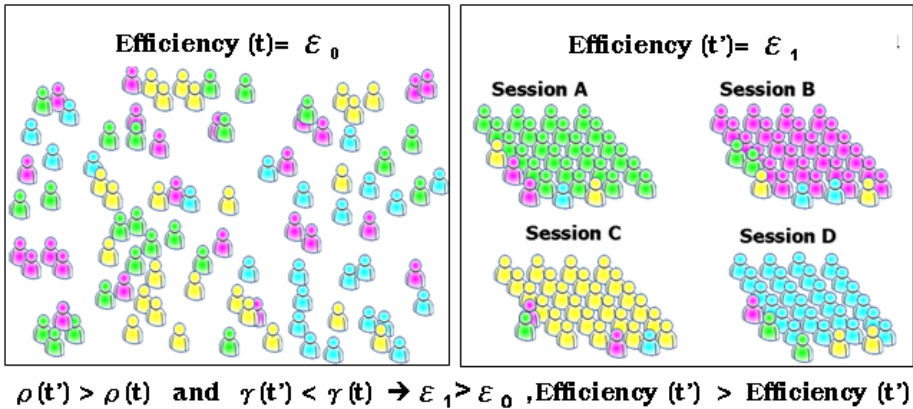


Fig. 1. Conference proximity e-service scenario

Assuming a proximity e-service environment is available in the conference, each participant has their own mobile device with facilities for exchanging information with others within a limited range. Individual mobile users manage their own information, including owner identity, scheduled presentations, copies of presentation slides, bibliographic references and URLs. Users can also provide research interest information and a list of colleagues/friends who are also attending the conference.

Mobile users can exchange information dynamically and spontaneously given physical proximity. In such contexts, individual physical encounters provide good opportunities for information exchange. Such information exchange can occur only during a limited period which can not be statically known. Owing to the limited communication time available during each encounter, it is important to rapidly access the most relevant information.

Some forms of collective wisdom can be generated. The group notes provide an example: all participants can take notes of their own or share notes with others. (For example, sharing notes with colleagues attending another session) During discussion

of conference sessions, participants can contribute their ideas for discussion by referring to their conference notes. Moreover, presenters can update their slides and make notes during discussions and share them with session participants. These personal notes can then be gathered in the form of group notes containing numerous heterogeneous viewpoints. These group notes may lead to extensive discussion regarding the social networks of individual participants simultaneously and participants can contribute some innovative thoughts. Colleagues and friends have similar interests particularly background domain. Those proximal participants may form strong tie clusters in the conference social network. The sessions include numerous network relationship clusters. The proximity of “cognitive view” (that is, participant homophily) may form weak tie relationships which will increase the effectiveness of information diffusion. The characteristics of proximity make it possible for those total strangers to treat others as familiar strangers and generate some collective efforts. Furthermore, collective wisdom is more likely to occur in a proximity e-service environment. Conference attendees may find some clues to connect to some unfamiliar people within the proximity e-service environment and carry out extensive collaboration.

Another form of collective wisdom is considered below. Andrew has just arrived at the conference. While registering at the conference, Andrew runs into his old friend and ex-colleague, Katrina, who is on her way to the same conference. They start talking about the research they are working on and decide that they would like to try to write a paper for another conference with a deadline in a few weeks. To plan their writing, they exchange current contact information, information about the conference, notes, documents, work pointers, and so on. This information is located on one or other of their mobile devices. Even though only a subset of these resources would normally be available to each other, they can still share the information they need for their collaboration.

Another example involves Katrina planning to publish a paper in another domain with which Andrew is not familiar. However, Andrew is familiar with an editor-in-chief who is also interested in this domain. Andrew thus sends an email to the editor and recommends Katrina’s work, and the editor then invites Katrina to join a research discussion. This relationship connects the isolated personal social networks and binds the strong tied relationship networks of individuals.

However, in proximity e-services all interactions occur within the context awareness environment. Contextual awareness means that private mobile user information may be exposed to others. In certain cases the anonymity of the owner of the information must be guaranteed, for example during an encounter between individuals who have previously never met and who do not want to know each other. In other situations the confidentiality of information to be transferred must be guaranteed.

The collective wisdom of ubiquitous proximity e-service environment comprises various levels. In ad-hoc ubiquitous e-service environments, even participants are not familiar with each other. UPS enables proximal e-service participants to contribute their experiences and form collective wisdom. Based on user preference or behavioral stereotype settings, UPS facilitates collective filtering which provides information to

identify trustworthy partners via an experience co-creation process. In such unfamiliar ad-hoc environments it is good to have information to serve as a reference for making good decisions.

Those ubiquitous proximity e-service cases have some common attributes that each participant just owns some pieces of information. Aggregate more information pieces will improve the decision quality, and then the collective wisdom will appear. Mobile and ubiquitous computing has changed its emphasis from “Anywhere, anytime” into “In this specific place, at this specific moment, for this specific person”, and pervasive communication is connecting proximal e-service participants to contribute ubiquitous collective wisdom.

5 Simulation Justification

The ubiquitous proximity e-service is designed to enhance the decision quality on trust evaluation via exploration of the collective wisdom of the surrounding user groups. In the ad-hoc e-service environment, a multitude of transactions take place between anonymous sellers and buyers. Since users do not have permanent identities, they have to handle the trust problem. Mostly, a seller deals with this problem by insisting on payment in advance, thereby, protecting himself from deceitful buyers. The seller delivers the service package only after receiving payment from the buyer. The buyer therefore must be confident of the seller’s willingness to deliver the service package.

Because the available e-service provision is highly dependent on the resources of the service provider, customers may not always get what they ask for. Aggressive sellers who are not able to provide requested services may decide to promote alternative choices, but customers may not want to waste their computational resources on annoying spam messages. After receiving the seller’s response, buyers have to decide whether to accept the provided choice. The interaction between the buyer and the seller can be formalized as a simple trust game.

The goal of simulation is to verify whether the collective wisdom gathered from ubiquitous environment could improve the decision quality for estimating the trustworthiness of unfamiliar user.

Healthy Environment vs. Malicious Environment. Lack of trustworthy infrastructure within the ad-hoc mobile e-service environment, each peer basically needs to maintain all threats in the environment on its own. Ubiquitous proximity e-service enables the collective wisdom from e-service participants and supports collaborative trust evaluation of nearby users. It should be expected that UPS could integrate available resources within an e-service environment to prevent malicious events. In order to evaluate the performance of UPS in various situations, we then set up three kinds of environments: Healthy Environment, Malicious Environment, and Neutral Environment. The “Healthy Environment” contains 80% honest users and 20% malicious users. On the contrast, the “Malicious Environment” contains 80% malicious users and 20% honest users. A “Neutral Environment” has half honest users and half malicious users as a benchmark for normal environment settings. We stabilize other parameter settings: there are 20 users within the e-service environment

with a balanced buyer-to-seller ratio. User behaviors are assumed in normal distribution within a normal resource level.

Figure 2 illustrates that use of UPS would help decrease cheat transaction rate. As interaction increases, the collective wisdom generated from participants’ co-experience would assist deter cheat transactions. The use of UPS is most effective in malicious environment – the cheat transaction rate could be lowered to 29% initially and would be down to 14% after 100 transactions take place. As in the “Healthy Environment”, with the use of UPS, cheat transaction rate would remain under 8% for the whole simulations and drop to 1% after 100 transactions take place. Simulation results indicate UPS’s collective wisdom mechanism would assist improve decision-making quality for all environment settings.

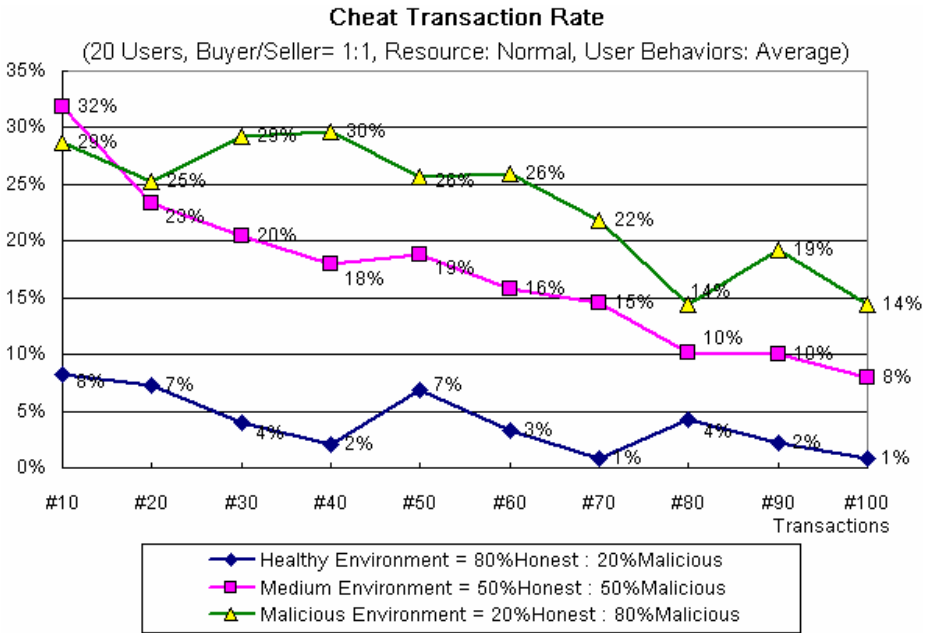


Fig. 2. Cheat transaction rate in Healthy/ Neutral /Malicious Environment

The simulation results clearly show that ubiquitous proximity e-service makes it possible for users to collaborate with the nearby user groups for establishing a reliable and trustworthy interaction environment. The ubiquitous proximity e-service realizes the collective wisdom and provides a feasible solution for quality decisions in the dynamic and distributed environment.

6 Conclusion

Ubiquitous e-service is one of the most recent links in the chain of evolution that has characterized the different eras of the internetworking environment. In order to leap

the trust barrier for the user to embrace these ubiquitous e-services, we present a ubiquitous proximity e-service for exploring collective wisdom in the ad-hoc ubiquitous environment. Simulation outcomes for trust decision quality enhancement show significant improvement in all kinds of environment settings. The ubiquitous proximity e-service makes it possible for users to collaborate with the nearby user groups for establishing a reliable and trustworthy interaction environment. It also facilitates and empowers the potential benefits of various ubiquitous e-service applications.

References

1. Allen, T.J.: *Managing the Flow of Technology*. MIT Press, Cambridge, MA (1977)
2. Anderson, B.: *Imagined Communities*. Verso, London (1983)
3. Aristotle: *The Nicomachean Ethics*. H. Rackham, translator. Harvard University Press, Cambridge, MA (1934)
4. Festinger, L., Schachter, S., Back, S.: *Social Pressures in Informal Groups: A Study of Human Factors in Housing*. Stanford University Press, Palo Alto, CA (1950)
5. Friedkin, N.E.: Information flow through strong and weak ties in intraorganizational social networks. *Social Networks* 3, 273–285 (1982)
6. Pór, G.: *The Quest for Collective Intelligence*. In: Gozdz, Kazmierz (eds.) *Community Building: Renewing Spirit & Learning in Business*, New Leaders Press, San Francisco (1995)
7. Granovetter, M.: The Strength of Weak Ties. *American Journal of Sociology* 78, 1360–1380 (1973)
8. Granovetter, M.: The strength of weak ties: A network theory revisited. In: Marsden, P.V., Lin, N. (eds.) *Social Structure and Network Analysis*, pp. 105–130. Sage, Beverly Hills, CA (1982)
9. Habermas, J.: *The structural transformation of the public sphere*. MIT Press, Cambridge, MA (1991)
10. Hwang, Y.C., Yuan, S.T.: A Privacy-Aware Identity Design for Exploring Ubiquitous Collaborative Wisdom. *LNCS*, vol. 4490, pp. 433–440. Springer, Heidelberg (2007)
11. Lazarsfeld, P., Merton, R.K.: Friendship as a social Process: A Substantive and Methodological Analysis. In: Berger, M., Abel, T., Page, C.H. (eds.) *Freedom and Control in Modern Society*, pp. 18–66. Van Nostrand, New York (1954)
12. McPherson, M., Smith-Lovin, L., Cook, J.: Birds of a feather: Homophily in Social Networks. *Annual Review of Sociology* 27, 415–444 (2001)
13. Plato. *Laws*. Plato in twelve volumes, Bury translator, vol. 11, p. 837. Harvard U. Press, Cambridge (1968)
14. Watts, D., Strogatz, S.: Collective Dynamics of Small-World Networks. *Letters to Nature* 393, 440–442 (1998)
15. Hill, R.A., Dunbar, R.I.M.: Social network size in humans. *Human Nature* 14(1), 53–72 (2003)

Obligations for Privacy and Confidentiality in Distributed Transactions

U.M. Mbanaso¹, G.S. Cooper¹, David Chadwick², and Anne Anderson³

¹ Informatics Research Institute (IRIS), University of Salford, UK

² Computing Laboratory, University of Kent, UK

³ Sun Microsystems Inc, Burlington MA USA

Abstract. Existing access control systems are typically unilateral in that the enterprise service provider assigns the access rights and makes the access control decisions, and there is no negotiation between the client and the service provider. As access management systems lean towards being user-centric, unilateral approaches can no longer adequately preserve the user's privacy, particularly where the communicating parties have no pre-existing trust relationships. Establishing sufficient trust is therefore essential before parties can exchange sensitive information. This paper describes a bilateral symmetric approach to access control which deals with privacy and confidentiality simultaneously in distributed transactions. We introduce the concept of Obligation of Trust (OoT) as a privacy assurance mechanism that is built upon the XACML standard. The OoT allows communicating parties to dynamically exchange their privacy requirements, which we term Notification of Obligations (NOB) as well as their committed obligations, which we term Signed Acceptance of Obligations (SAO). We describe some applicability of these concepts and show how they can be integrated into distributed access control systems for stricter privacy and confidentiality control.

1 Introduction

Trends in emerging access management systems raise an interesting paradox. On the one hand, service providers' applications require identity/attribute related information in order to validate a user's request. On the other hand, users may not wish to disclose their information or attributes to a remote Service Provider (SP) without determining in advance whether the service provider can be trusted to comply with their privacy preferences. Conventionally, privacy is often considered from the users' perspective, just as access control is considered from the SP's standpoint. That is, the user is concerned about the confidentiality of their personal identifying information (PII), and the resource provider is concerned about the confidentiality and integrity of the resource information. These assumptions have resulted in unilateral asymmetric approaches. Yet the SP may also have sensitive attributes such as membership certificates of consortia, or trust relationships with third parties (TTPs) or policies of various kinds that a resource user may demand to see before releasing their PII. This suggests a symmetrical approach may be more appropriate, and has led to the research

topic called trust negotiation where each party's attributes are released incrementally to the other, as trust is established between them [1]. In B2B transactions, both parties may require the dynamic exchange of service level agreements (SLA) or business level agreement (BLA) in order to assess the mutual benefits and associated risks. This may also require the establishment of trust and a guarantee of compliance to agreed business rules. One way to achieve this is for each party to issue to the other a proof of acceptance of the requirements contained in the SLA or BLA. Enabling the runtime exchange of these requires a bilateral symmetric approach to allow the communicating parties to indicate their willingness to accept constraints imposed by the other party, before the latter is prepared to reveal their sensitive information. There is therefore some overlap between user privacy requirements and business requirements.

To address confidentiality and privacy problems simultaneously and symmetrically, the parties in distributed transactions should have a standard means of declaring their privacy requirements and the respect they will give to the other party's privacy requirements before sharing their resources. All parties need to evaluate the risk of giving out their PII and determine the degree to which they are prepared to trust the other participating actors. They will need to identify any constraints and obligations they may wish to place on the others. Trust negotiation [1] has been proposed to address this dilemma, but as will be pointed out later it has its limitations. We therefore approach the subject of resources control in a slightly different manner. We propose a technical solution that derives its concepts from well established standards. We describe the concept of an Obligation of Trust (OoT) protocol, whereby two parties can exchange difficult-to-repudiate¹ digitally signed *obligating constraints* (or Notification of Obligations (NOB) which detail their requirements for sending their sensitive information to the other party), and *proof of acceptances* (or Signed Acceptance of Obligations (SAO), which acknowledge the conditions they have accepted for receiving the other party's sensitive information). The OoT protocol provides the negotiating mechanism for carrying obligating constraints and proof of acceptances between security domains. Being signed, they help the communicating parties to produce difficult-to-repudiate technical evidence in the event of disputes. The OoT protocol also provides a mechanism for dynamically exchanging other obligating documents such as service level agreements (SLAs), business level agreements (BLAs), contractual documents, etc. In effect, the OoT protocol merges technical solutions (mechanical exchange and matching, digital signature) with potential social/judicial solutions (non-repudiation, technical legal recourse). The rest of this paper is structured as follows. Section 2 describes related research. Section 3 presents the OoT protocol as well as how matching of obligation constraints and proof of acceptances is achieved. Section 4 describes the system architecture of a reference engine and its core subsystems, which we are currently constructing. In section 5, we provide an example use of the model and section 6 concludes the paper.

¹ We use the term "difficult-to-repudiate" rather than non-repudiation, since repudiation is a legal issue that has to be determined in a court of law. The technical constructs proposed in this paper should make it more difficult for an entity to repudiate their actions.

2 Related Research

The Platform for Privacy Preferences (P3P) [2] is one approach that attempts to address privacy in commercial service provider (SP) websites. Whilst it has provided some degree of privacy awareness, it has not particularly addressed privacy concerns in distributed access control systems. The fact that P3P is widely implemented by most websites and processed by compliant user-agents by comparing the P3P policy statement against an APPEL [3] statement that describes the user's privacy preferences is beneficial. By contrast, in distributed access control systems, SPs don't usually convey their privacy policy statements to the service users during access request. Even if a user in a distributed access control system retrieves the remote P3P policy, the policy may not necessarily meet the user's preference. Thus, the user may abort the service or continue without the choice for further negotiations. Also P3P doesn't support provider-side requirements; the SP may have some privacy constraints that require enforcement at the client's side. The main components of a P3P privacy statement include the *recipient* of the data, the *purpose* for which that data is requested, the *retention period* at the collector's store, and the *data category*. It can include other components such as *disputes* and *remedies*, as well as whether *disclosure to third parties* is allowed. Though P3P covers most of the basic principles of privacy [4], the fact that it has not satisfactorily resolved the requirements for bilateral privacy negotiation [5] limits its use in access control.

Shibboleth [6] from Internet2 provides a mechanism for federated access management based on the SAML security standard [7]. Shibboleth provide single sign on (SSO) and a mechanism for an IdP in one security domain to securely convey attributes about a web-browsing user to a SP in another security domain. In Shibboleth, privacy is addressed in two ways. Firstly, after the user authenticates to the IdP, the Shibboleth authentication service generates a one time handle to identify the user and transmits this to the SP. Secondly, the IdP uses Attribute Release Policies (ARPs) to decide whether to release specific attributes to the SP or not. This is fine as long as the remote site doesn't require any identifying attributes to complete the service. But this is unlikely to be the case in most transaction scenarios. Furthermore, the Shibboleth infrastructure doesn't provide any support for bilateral negotiation of service parameters. If the user doesn't provide the requested attributes, access to the services is unilaterally denied. Another significant privacy flaw is that the ARP is coarse and doesn't support most of the known privacy principles [4].

ID-WSF from the Liberty Alliance is an open standard for federated identity management that is built upon the extensibility of SAML security assertions [7]. It provides a framework for the discovery and communication of identity information among federated domains. When a client authenticates to an IdP, a SAML-based assertion handle (SSO) is generated and communicated to a relying party or SP with optional information which the relying party may use to call-back the user's IdP. The ID-WSF framework provides a flexible security model for a highly distributed set of IdPs.

Microsoft, IBM and VeriSign have been working on a set of specifications (called "WS-Security roadmap" or "WS-Identity Policy Framework") for their next generation platform of Web services. The WS-Policy suite of policies, which includes

Security Policy, Reliable Messaging Policy, etc. are not designed primarily for implementing access control. They are predominantly designed to enable Services to advertise what requirements (especially authorization requirements) a requesting party must satisfy in order to use the services. The idea is that a requesting party can consider what it is willing and able to accept, before sending attributes that can satisfy the requirements. However, WS-policies do not necessarily provide a means to enforce access control policies since typically they are not to be consumed by Policy Decision Points (PDPs).

One approach that addresses bilateral access control is the Automatic Trust Negotiation (ATN) technique [8, 9]. ATN introduces a trust negotiation layer for symmetrical interactions. Research efforts in this area have developed advanced ATN techniques to cover a variety of scenarios [10] [11] [12]. Recent initiatives in preserving privacy [13, 14] also favour the use of negotiation techniques for solving privacy problem. ATN is an access control technique that permits the gradual release of policies and credentials so that trust can be incrementally increased until the communicating parties are sufficiently satisfied of each others trustworthiness to send all their confidential information. However, ATN doesn't provides mechanisms whereby the relying party can convey proof of acceptance for obligating constraints - assurance that the attributes contained in the assertions will be used in accordance with the party's privacy preferences. Recent work in this area by Spantzel et al [15] introduces a framework that integrates ATN with Identity Management Systems (IdM). Based on their comparison of ATN and IdM systems, it shows that ATNs have not truly explored access security standards such as XACML, SAML, etc which may limit their practical implementation.

To the best of our knowledge, none of the above systems provides a mechanism for the remote enforcement of privacy obligations. So there is uncertainty that the receiving party will adhere to them. Further, the receiving party may not accept any liability if the sender's PII is compromised. Without privacy assurances there is the possibility that the receiving party may even misuse the sender's PII without any form of liability. Privacy negotiation will provide a mechanism that relies less on trusted external third parties and more on the communicating parties themselves. Privacy is governed by laws, legislation and principles requiring that privacy solutions should provide tenable difficult-to-repudiate technical evidence in the case of a privacy dispute. Consequently, there is a need to provide a mechanism for providing tamper-proof technical evidence that may be used in the event of disputes when parties do not conform to their commitments. One approach to achieve this is to provide a protocol to enable participating parties to exchange digitally signed commitments. We acknowledge that a technical "non-repudiable signature" on its own may not be sufficient evidence for a court of law since other factors also contribute to a digital signature being legally non-repudiable, such as: how much active participation the user had in deciding to sign, how free the user is to use the signed-for sensitive information, whether the software automatically generated the signature, and how complex the signed agreement is. However, these legal issues are not within the scope of the current paper. We consider the technical issues only that will help to provide difficult-to-repudiate evidence.

3 Obligation of Trust (OoT) Protocol

Obligation of Trust is a protocol that defines a standard mechanism enabling two or more communicating parties to exchange *obligating constraints* as well as *proof of acceptances*. The basic concept is built upon the assumption that a requesting party has no means of enforcing obligations placed on a remote party. In traditional access control systems, an obligation is an action that should be performed by a Policy Enforcement Point (PEP) in conjunction with the enforcement of an access control decision [13]. XACML [16] describes an *Obligation* element as a set of attribute assignments, with an attribute *FulFillOn* which signifies whether the consuming PEP must fulfill the *obligation* if the access control decision is “Permit” or “Deny”. When a Policy Decision Point (PDP) evaluates a policy containing obligations, it returns the access control decision and set of obligations back to the PEP. However, in a distributed environment the SP’s PEP is unlikely to be in the same security domain as the service requestor; therefore there is no guarantee that any obligations required by the requestor can either be incorporated into the policy used by the SP’s PDP, or even if they can, be enforced by the SP’s PEP. Given this, it makes sense to address the remote enforcement of obligations by allowing a SP to convey back to the requestor an acceptance or rejection of their obligating constraints. The OoT protocol addresses this interaction. We divide the OoT protocol into two steps: Notification of Obligation (NOB) (which may be signed or unsigned) and Signed Acceptance of Obligation (SAO) (which must be signed). The OoT protocol is symmetric. An initiating party sends a NOB outlining the obligating constraints it is placing on the other party and the commitments it is willing to make if the other party accepts its obligations. The other party, after evaluation, sends back either a signed acceptance (SAO) of the constraints it accepts and the commitments it requires, or initiates more service negotiations with its own NOB, or rejects the request and terminates the session. Because the NOB and SAO are constructed using standard XACML obligations elements, both communicating parties have a common language for expressing their requirements and commitments, and are able to feed these obligations directly into their PDPs for automatic decision making, and ultimate enforcement by their respective obligations services.

OoT Encoding Scheme

The Web Services Profile of XACML (WS-XACML) [17] describes a way for carrying XACML policies between communicating parties. WS-XACML specifies formats for four information types:

- an authorization token or credential for carrying an authorization decision across realms,
- a policy assertion type that is based on XACML elements which can embed WS-Policy or other XML constructs,
- ways to wrap P3P policy preferences and match them using XACML assertions, and
- XACML Attributes in SOAP Message Headers in such a way that they can be authenticated as having been issued by a trusted authority.

The WS-XACML Assertion Type is an abstract framework that describes an entity’s Web Service’s policy in the context of different policy domains, such as authorization or privacy domains. The name of the Assertion’s element indicates the domain to which it applies, such as XCMPLPrivacyAssertion for the privacy domain and XACMLAuthzAssertion for the authorization domain. The XACMLPrivacy Assertion deals with privacy specific Assertions which can carry Requirements i.e. what the asserter requires of the other party, and Capabilities i.e. what the asserter is willing and able to do for the other party if its Requirements are satisfied. The inner box in Figure 1 depicts the WS-XACML model which defines an *XACMLAssertion AbstractType*. This allows constraints on a policy vocabulary to be expressed as XACML Apply functions. The *XACMLAssertion* contains two sets of constraints as shown in figure 1. The first set, called *Requirements*, describes the information or behavior that the policy owner requires from the other party. The second set, called *Capabilities*, describes the information or behavior that the policy owner is willing and able to provide to the other party. One instance of this type is the *XACMLPrivacyAssertion* whose *Capabilities* element describes the *Obligations* that are being accepted and the information that will be provided. The *Requirements* element specifies the *Obligations* that the sender requires of the other party in order to proceed.

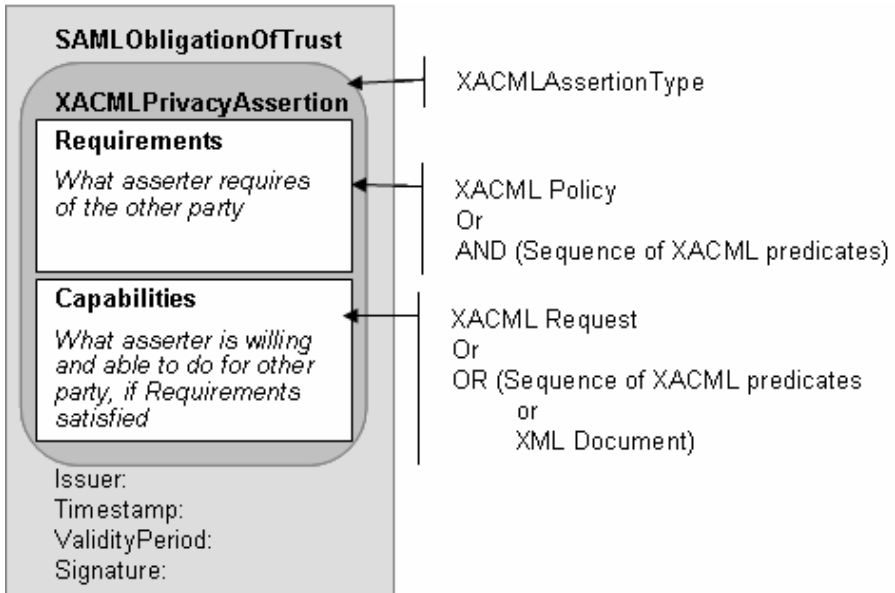


Fig. 1. SAML Obligation Of Trust Model

Using the built-in extensibility mechanism of WS-XACML and SAML Assertions, we can conveniently encode the components of the OoT protocol as extensions of standard elements. The NOB can be expressed as an instance of a *XACMLPrivacy Assertion* in which the desired obligating constraints are placed in the *Requirements*


```

<Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:xpath-expression-subset">
  <AttributeSelector
    RequestContextPath="//P3P10/POLICIES/POLICY/STATEMENT/PURPOSE/*"
    DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression" />
  <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:xpath-expression-bag">
    <AttributeValue DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-
      expression">//P3P10/POLICIES/POLICY/STATEMENT/PURPOSE/current</Att
      ributeValue
    <AttributeValueDataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-
      expression">//P3P10/POLICIES/POLICY/STATEMENT/PURPOSE/admin</Att
      ributeValue>
    <AttributeValueDataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-
      expression">//P3P10/POLICIES/POLICY/STATEMENT/RECIPIENT/ours</Att
      ributeValue>
  </Apply>
</Apply>

```

Fig. 2. Example of WS-XACML constraint on P3P PURPOSE

section of the Assertion, and any obligations that the sender is willing and able to fulfill in the *Capabilities* section. The SAO can be expressed as an instance of a *XACMLPrivacyAssertion* in which the *Requirements* section specifies the sender's understanding of what the recipient has committed to do and the *Capabilities* section specifies the obligations that the sender has committed to undertake. By signing the SOA the signer is stating in a difficult-to-repudiate form their commitment to fulfill the *Obligations* contained in the *Capabilities* element, so long as their *Requirements* are satisfied. Figure 1 shows the extensions of WS-XACML and SAML that map into our Obligation of Trust model. The OoT schema is available at [18], but basically it defines a new SAML protocol request type (the Obligation of Trust Query Type) and a new SAML statement type (the Obligation of Trust Statement Type).

In the privacy domain, these elements can be used to describe either the acceptable (Requirements) or supported (Capabilities) P3P policy contents. For example, if a recipient will only use the sender's sensitive information for the "current" transaction and "admin" purposes, and the information is only for the designated recipient, this can be sent as a P3P policy STATEMENT of PURPOSE expressed as a WS-XACML constraint as shown in figure 2.

OoT Protocol Scheme

Figure 3 is a simplified sketch of the OoT protocol in operation, and shows how two parties may exchange signed components of the OoT. Party A wishes to access item X from party B, but it is assumed that party A knows nothing about the privacy or access control requirements for item X. Similarly, Party B knows nothing about the privacy requirements of Party A's attributes. Party A sends a request for item X and Party B responds with a NOB containing its *Requirements* and *Capabilities*. Figure 4 shows an outline of an algorithm for the decision making when a party receives a NOB. Party A checks whether it can satisfy Party B's *Requirements*, and whether

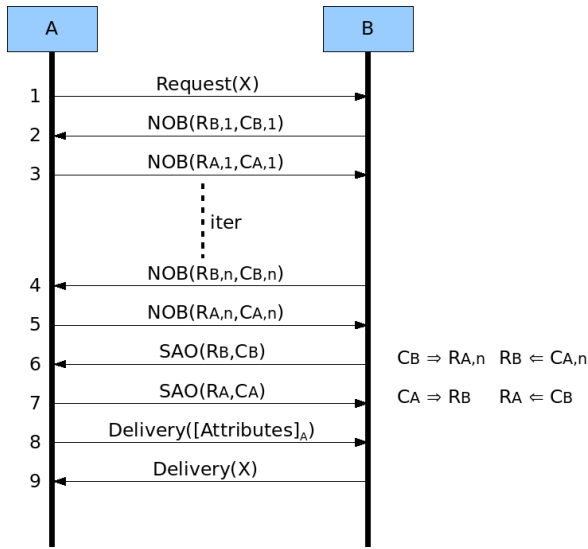


Fig. 3. The OoT Protocol Sketch

party B's *Capabilities* can satisfy its own (party A's) *Requirements*. If Party B's *Capabilities* are acceptable and sufficient for Party A, and A can fully meet B's requirements, then A can send an SAO to B stating its pick of the offered capabilities and its own capabilities to meet party B's requirements. If B's capabilities are acceptable but not sufficient, or A has additional requirements, A may send a counter NOB to B containing its additional or alternative *Requirements*. A's *Requirements* will determine the subset of B's *Capabilities* that it requires, and A may supplement them with additional ones of its own. A's *Capabilities* will include the subset of B's *Requirements* that it can provide, along with any additional ones it may be willing to provide. If Party B's *Capabilities* are insufficient for Party A, then A will either terminate the session or return a NOB with *Requirements* that supercede B's stated *Capabilities*. If A cannot meet all the stated requirements of B, then A may decide to terminate the session or add a reduced set of *Capabilities* to the NOB.

Party B evaluates party A's NOB and if satisfied with A's *Capabilities* and *Requirements* it returns a signed SAO stating in its *Capabilities* that it can fulfill all of party A's *Requirements*, and in its *Requirements* which of Party A's *Capabilities* it has chosen. If B is satisfied with A's *Capabilities* but not with A's *Requirements*, B may either send another NOB to A showing less *Capabilities* than A requires (along with its own *Requirements*), or terminate the session. If B is not satisfied with the *Capabilities* of A's NOB, it will either terminate the session or return a NOB with increased *Requirements*. If Party A receives another NOB, and this is satisfactory, it returns a signed SAO, otherwise it behaves as last time around. If Party A receives party B's SAO, and if satisfied with it, it returns its own signed SAO. Thus the parties continue to exchange NOBs until either one party terminates the session (negotiated agreement not possible) or returns a signed SAO. Once a signed SAO has been delivered the recipient must either accept this by returning its own signed SAO or

- Set flag initially to “SAO”
 - Evaluate received requirements to determine whether I can meet them with my capabilities
 - If so, construct offered Capabilities to match received requirements
 - If not, either
 - terminate or
 - determine* whether additional capabilities should be offered to match, and/or
 - construct capabilities to match a subset of the received requirements, plus additional alternative capabilities to be offered, and set flag to “NOB”
 - Analyse capabilities to be offered by me (as determined above) and construct a revised list of (my) requirements.
 - Analyse sets of capabilities received and compare with my list(s) of requirements (as determined above).
 - If all my requirements are met from one set of offered capabilities, keep the above-defined requirements.
 - If all my requirements are met from merged sets of offered capabilities, construct Requirements from these, set flag to “NOB”
 - If my requirements are not met, either
 - terminate or
 - determine* whether requirements can be relaxed due to alternative capabilities being offered and modify requirements accordingly and set flag to “NOB”
 - If SAO flagged, send SAO, else send NOB.
- (* “determine” could include the possibility to ask a human operator.)

Fig. 4. Outline Algorithm for handling a NOB

terminate the session. It is not allowed to return a NOB in response to a signed SAO, since this is in effect rejecting what one had previously offered in a prior protocol exchange. Once the negotiation is complete, and each party is in possession of the signed SAO of the other party, then Party A delivers the attribute values defined in Requirement B and Party B delivers item X to A.

As indicated above, in some transactions it will be the case that either a user’s configured capabilities are insufficient to match an SP’s requirements, or a user’s requirements are too great for an SP’s capabilities. In this case the software might indicate to the user that the SP’s (or user’s) requirements are not covered by any of the user’s (or SP’s) sets of capabilities. The user should be able to view the NOB request and possibly extend their capabilities or reduce their requirements. As an example, suppose a user has configured his requirement’s policy so that recipients are not to reveal the user’s PII to 3rd parties, but a Service X offers very generous compensation to Service C’s users who are willing to sign up for X’s new services. In this case, Service C could send the user a NOB containing a *Requirement* to provide permission for Service C to release PII to Service X, in exchange for compensation. The user’s agent does not have a *Capability* to match this *Requirement*, so the user’s

client software could display Service C’s *Requirement* for the granting of permission to forward the PII to Service X, along with Service C’s *Capability* to offer compensation to the user. If the user dynamically chooses to accept this contract, a new *Capability* is added to the user’s set of XACMLPrivacyAssertions, for this and future use, and a signed SAO is sent to Service C.

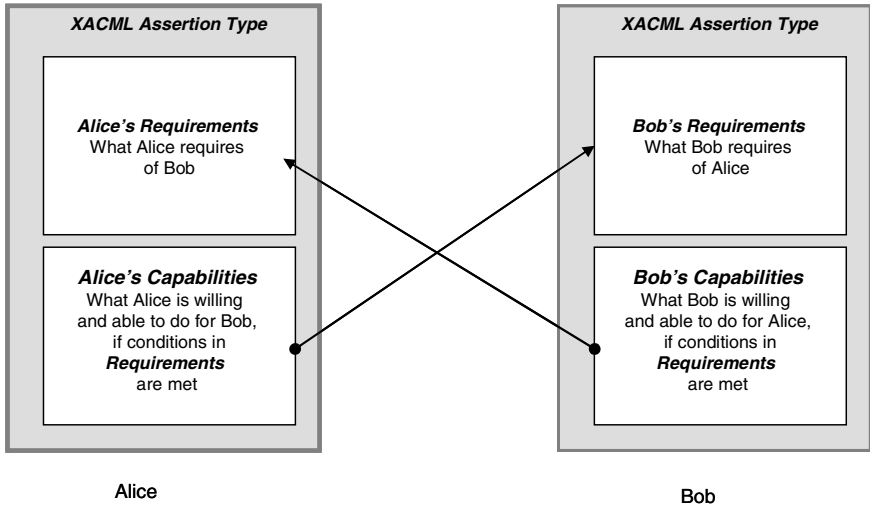


Fig. 5. Matching of Two WS-XACML Assertion Type

Matching and Evaluation

Requirements are logically connected by AND: the policy owner requires the other party to satisfy **all** of the constraints listed in the *Requirements* section. *Capabilities* on the other hand are logically connected by a non-exclusive OR: the policy owner is willing and able to provide any subset of the capabilities described by these constraints. Figure 5 illustrates the matching of the two WS-XACML Assertions. Two *XACML Assertions* match if, for each assertion, all constraint in the *Requirements* section are satisfied by (at least) one of the statements in the *Capabilities* section of the other assertion. WS-XACML specifies efficient generic algorithms for determining that one constraint “satisfies” another. We can use this mechanism to evaluate an XACML-P3P policy against an XACML privacy profile (or any policy expressed in XML), provided we have matching semantics between them. Once the matching is done, the next step is to extract the capability that matches the recipient’s requirements, produce the SOA and generate the signatures.

4 Example of WS-XACML Aware Applications

The OoT protocol provides a platform which permits two or more communicating parties to negotiate obligating constraints in a tamper proof manner. Privacy Negotiation is one such good example of using the OoT principles.

As an example, an Internet-based ticket service (ITS) provides online ticketing services to both consumers and partners through automated Web services. The ITS can provide special price offers to certain categories of clients in particular seasons. The ITS requires prospective clients to provide or show proof of possession of certain properties and then to make firm commitments that they will not disclose its price list to third parties (i.e. competitors) before it can decide whether they qualify for special offers. On the other hand, the clients may not wish to give out their sensitive attributes without receiving proof from the ITS that it will not disclose them. The ITS therefore needs to assure the clients that their attributes will be held according to their privacy preferences. Figure 6 depicts the ITS's internal XACMLPrivacyAssertion and

| |
|--|
| <p>XACMLPrivacyAssertion (ITS)</p> <p>Requirements</p> <ul style="list-style-type: none"> Client Name IATA membership certificate Certified Quarterly Sales > £12,000.00 Price List not given to 3rd parties <p>Capabilities</p> <ul style="list-style-type: none"> PURPOSE: PII used internally for this transaction RETENTION: PII kept only until transaction is completed RECIPIENT: PII not given to any 3rd party |
|--|

Fig. 6. ITS's Internal XACMLPrivacyAssertion

| |
|---|
| <p>XACMLPrivacyAssertion (customer)</p> <p>Requirements</p> <ul style="list-style-type: none"> RETENTION: PII kept only until transaction is completed RECIPIENT: PII not given to any 3rd party <p>Capabilities</p> <ul style="list-style-type: none"> Name IATA membership certificate Certificate of Incorporation Certified Quarterly Sales > £12,000.00 Price List not given to 3rd parties |
|---|

Fig. 7. Customer's Internal XACMLPrivacyAssertion

figure 7 is the customer's internal XACMLPrivacyAssertion. Looking at the assertions, the customer's *Requirements* are really "Obligations" to be fulfilled by the ITS. Similarly, the ITS's *Capabilities* are really "Obligations" that the ITS is able and willing to meet. The OoT provides the mechanism to assure each participant of the other's commitment to respecting their security preferences. Each party can save the digitally signed XACMLPrivacyAssertion with the complete *Capabilities* as difficult-to-repudiate evidence in the case of disputes.

5 Conclusion

This paper describes one concrete approach to enhancing privacy assurance, by permitting the bilateral exchange of privacy *Requirements* and the *Capabilities* to satisfy them. The OoT mechanism merges technical solutions with possible social/judicial solutions for security assurance in distributed open systems. This mechanism demonstrates a secure way of using P3P policies in WS-XACML which provides a framework for the dynamic exchange of requirements and capabilities, meaning that this framework can support the P3P platform with minimal effort. Our solution demonstrates significant improvement in the provision of privacy in distributed transactions where technically “difficult-to-repudiate” services are vital. Again, the benefit of this framework is that the same security engine can apply to the four types of information described in WS-XACML, meaning that privacy and confidentiality can be achieved simultaneously for both service providers and consumers. This approach is currently being implemented.

An additional benefit of this approach over traditional ATN is that it has the potential to reduce the number of interactions between parties and therefore the effects of network latency since both requirements and capabilities can be transmitted in a single payload rather than separately. A mechanism that assures each party that their information will be used in accordance with their wishes will increase the level of trust and confidence between the communicating parties and may even reduce the liabilities of regulated organizations.

The OoT protocol has a couple of limitations. Firstly it assumes that the other party exists as a physical entity that can be sued if violations occur. This requires either a robust PKI system to exist or some other mechanism to establish whether the subject of a certificate is a legal entity, and will put meaningful identifying information in the issued certificate. Secondly, it is open to probing attacks. A malicious party can probe another party by providing bogus capabilities in order to gather the other party’s requirements and capabilities and then terminate the connection before any actual data is transferred. In [19], we described how XACML can be used to address the probing attack by a trust negotiation involving the gradual and incremental exchange of information. This requires that the XACML policy is expressed in such a way that the level of trust established can determine what other information (policy/attributes) is released at any phase. The order and sequence are controlled by the crafting of policy rule expressions. Furthermore, we have not dealt with refinements for multiple assertions and multiple set of Capabilities. These are the subject of further work.

Work is currently being carried out on a reference implementation of the proposed approach, and the testing and evaluation of this will be published in due course.

References

1. Bertino, E., Ferrari, E., Squicciarini, A.: Trust Negotiations: Concepts, Systems and Languages, pp. 27–34. IEEE Computer, Los Alamitos (2004)
2. W3C: The Platform for Privacy Preferences 1.0 (P3P 1.0). Technical Report (2002)
3. Langheinrich, E.Z.M.: A P3P Preference Exchange Language 1.0 (APPEL1.0). W3C (April 5, 2002)

4. OECD: Fair Information Practice. In *The Electronic Marketplace A Report To Congress* (May 2000), <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>
5. W3C: Platform for Privacy Preferences (P3P) (2004)
6. Cantor, S.: Shibboleth Architecture. Internet2 Middleware (2005), <http://shibboleth.internet2.edu/shibboleth-documents.html>
7. Cantor, S., Kemp, J., Philpott, R., Maler, E.: Security Assertion Markup Language (SAML) V2.0 (March 2005), <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
8. Seamons, K.E., Ryutov, T., Zhou, L., Neuman, C., Leithead, T.: Adaptive Trust Negotiation and Access Control. In: *10th ACM Symposium on Access Control Models and Technologies*, Stockholm, Sweden (2005)
9. Winsborough, W.H., Li, N.: Towards Practical Automated Trust Negotiation. In: *Policy 2002. Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks* (2002)
10. Seamons, K.E., Winslett, M., Yu, T., Yu, L., Jarvis, R.: Protecting Privacy during On-line Trust Negotiation. In: *2nd Workshop on Privacy Enhancing Technologies*, San Francisco, CA (2002)
11. Winsborough, W.H., Seamons, K.E., Jones, V.E.: Negotiating Disclosure of Sensitive Credentials. In: *2nd Conference on Security in Communication Networks*, Amlfi, Italy (1999)
12. Bertino, E.F.E., Squicciarini, A.: TNL: An XML-based Language for Trust Negotiations. In: *IEEE 4th International Workshop on policies for Distributed Systems and Networks*, Lake Como Italy (2003)
13. Pau, L.-F.: Privacy Negotiation and Implications on Implementations. In: *W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement* (2006)
14. Preibusch, S.: Privacy Negotiations with P3P. In: *W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement* (2006)
15. Spantzel, A.B., Squicciarini, A.C., Bertino, E.: Trust Negotiation in Identity Management. *IEEE Security & Privacy*, 55–63 (2007)
16. OASIS: eXtensible Access Control Markup Language (XACML) Version 2.0. OASIS Standard (February 1, 2005)
17. Anderson, A.: Web Services Profile of XACML (WS-XACML) Version 1.0, WD 8. OASIS XACML Technical Committee (December 12, 2006)
18. University of Salford: Schema for Obligation of Trust (OoT) (December 2006), <http://infosec.salford.ac.uk/names/oot/ootSchema/>
19. Mbanaso, U., Cooper, G.S., Chadwick, D.W., Proctor, S.: Privacy Preserving Trust Authorization using XACML. In: *TSPUC 2006. Second International Workshop on Trust, Security and Privacy for Ubiquitous Computing*, Niagara-Falls, Buffalo-NY (2006)

Multi-channel Enhancements for IEEE 802.11-Based Multi-hop Ad-Hoc Wireless Networks*

YongSuk Lee¹, WoongChul Choi^{1,**}, SukJoong Kang¹, and SeongJe Cho²

¹ Department of Computer Science
KwangWoon University

² Division of Information and Computer Science
DanKook University
wchoi@kw.ac.kr

Abstract. Collision avoidance is critical for the performance of contention-based medium access mechanism such as CSMA. In this paper, the IEEE 802.11-based MAC protocol is enhanced for performance improvements in multi-hop ad-hoc wireless networks. The protocol behavior of hidden terminals in carrier sensing range[10] is important for end-to-end performance. There are several mechanisms defined in IEEE 802.11 standard such as IFS(Inter Frame Space), but we address a problem that such time interval is not long enough to avoid unnecessary collisions by the hidden terminals in carrier sensing range. We have conducted a comprehensive simulation to study performance improvement. The simulation results indicate that the performance is increased and the number of the dropped packets due to unnecessary collisions can be significantly reduced as much as a half.

Keywords: Ad-hoc wireless networks, IEEE 802.11, MAC, Collision, CAI (Collision Avoidance Interval).

1 Introduction

In the IEEE 802.11-based MAC protocol[1], two medium access control protocols are specified - PCF(Point Coordination Function) and DCF(Distributed Coordination Protocol). DCF is often used as a referred scheme for multi-hop ad-hoc wireless networks, and is a contention-based medium access protocol - a host that has frames to send can send them only when the medium is available, which means it works in simplex mode. There are several research works to overcome this limitation[7][8][9].

The range covered by the power necessary for transmitting a frame has two disjoint areas, named transmission range and carrier sensing zone (Fig. 1)[10]. In transmission range, a node can sense and decode a signal correctly, whereas a node can sense but can not decode it correctly in carrier sensing zone. To avoid a collision, a node is

* This work was supported by the Korea Science and Engineering Foundation(KOSEF) grant funded by the Korea government(MOST) (R01-2005-000-10934-0) and by the Research Grant of KwangWoon University in 2007.

** Corresponding author.

required to sense the medium first before transmitting a frame. If it finds the medium busy, the behavior of the node in IEEE 802.11 specification is as follows. If the node is in transmission range, it can decode the signal correctly, so it can also recognize NAV(Network Allocation Vector) which indicates the remaining time of on-going transmission sessions, therefore, it defers transmitting a frame during that NAV interval. But if it is in carrier sensing zone, the node can not decode the signal, so it can not recognize NAV.

In this paper, we address the importance of the protocol behavior in carrier sensing zone and show that the behavior is required to be modified to avoid unnecessary collisions to improve performance. With these modifications on MAC protocol, we show how significantly the performance improves by both in-depth analysis of the protocol behavior and simulation. We use the term of packet and frame interchangeably in this paper, although the former is usually used for layer 3 terminology, and the latter for layer 2[14], and if the distinction is required, it will be clarified in the context.

The rest of this paper is organized as follows. In Section 2, we review the related works. We provide the problem statements in Section 3 and detailed description of our solution in Section 4. In Section 5 and 6 discusses simulation and the results. We conclude the paper in Section 7.

2 Related Works

There have been many research efforts to improve the performance of the IEEE 802.11-based wireless networks. The efforts can be categorized into the collision avoidance in terms of power control for transmitting a packet, hidden/exposed terminal problem and how to handle a collision. Jung *et al.* [10] propose a power control protocol where MAC protocol uses a maximum power level for RTS-CTS and a minimum power level for DATA-ACK, combined with using a maximum power level for DATA periodically to avoid any potential collision and show the throughput and power saving improvement. Fujii *et al.* [11] propose a MAC protocol where a high-power node forwards the RTS and CTS packets from a low-power node to improve success rate performance of a data, by reducing collisions that occur after connection establishments, regardless of the size of the transmission range. Dutkiewicz [12] tries to find out the optimum transit range to maximize data throughput in ad-hoc wireless networks. The author presents a simulation study that under a wide set of network and load conditions multi-hop networks have lower performance than single-hop networks, data throughput is maximized when all nodes are in range of each other and also shows that the addition of relay-only nodes does not significantly improve throughput performance of multi-hop networks. Bharghavan *et al.* [5] investigate a hidden/exposed terminal problem in a single channel wireless LAN. They modify the basic binary exponential backoff algorithm for fair use of bandwidth. They examine the basic RTS-CTS-DATA message exchange, classify the hidden/exposed terminal problem in four cases and propose solutions for each case. In [9], Bharghavan proposes Dual Channel Collision Avoidance (DCCA), which employs two channels for signaling and data in order to avoid collisions efficiently in all cases of hidden/exposed receivers and senders, and Fair Collision Resolution Algorithm (FRCA), which seeks to fairly resolve collisions with both consideration for spatial locality of

stations and back-off advertisement, in order to provide better channel utilization and delay properties compared to IEEE 802.11 standard. Cali *et al.* [6] propose a method that estimates the number of active stations via the number of empty slots, and exploit the estimated value to tune the contention window value based on their analytic model. Kwon *et al.* [3] propose a fast collision resolution(FCR), which actively redistributes the backoff timer for all competing nodes, thus allowing the more recent successful nodes to use smaller contention window and allowing other nodes to reduce backoff timer exponentially when they continuously meets some idle time slots, instead of reducing backoff timer by 1 after each idle time slots, as in the original IEEE 802.11 DCF. FCR can resolve collisions more quickly than 802.11 DCF. Lin *et al.* [4] propose a mechanism called distributed cycle stealing for improving the performance of DCF protocol of 802.11. They investigate the issue of efficient channel utilization, where all the communications should obey power-distance constraints, which guarantee that all transmissions would not disturb each other during all communication periods. Acharya *et al.* [8] propose the Data-Driven Cut-Through Medium Access(DCMA) protocol, which combines the ACK to the upstream node with the RTS to the downstream node in a single ACK/RTS packet to reduce collision and forwarding latency.

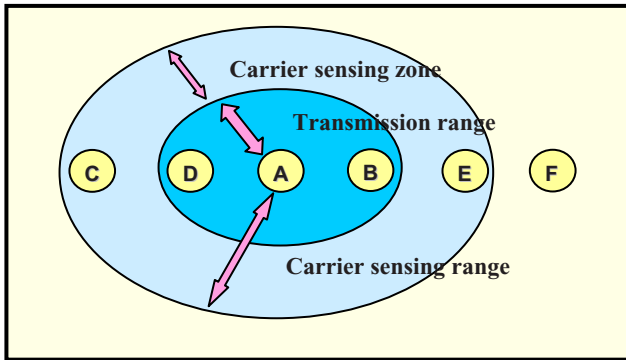


Fig. 1. Two disjoint areas of carrier sensing zone and transmission range, both of which constitute the carrier sensing range for node A. We assume that node A is a sender and node B is a receiver and transmission range from a frame transmitting source is one hop and carrier sensing range is two hops. Then node C and E is said to be in carrier sensing zone of the sender side.

3 Problem Statement

Consider a simple fixed chain topology like Fig. 1. Assume that node A is a sender, node B is a receiver and all the other nodes have data frames to send. Suppose that node A initiates a frame transmission to node B with RTS-CTS-DATA-ACK mechanism. Fig. 2 shows how 802.11 protocol proceeds for each node and how collision occurs.

In that situation, node D is in transmission range when node A sends RTS to node B. Likewise, node E is in transmission range when node B answers CTS to node A.

Therefore, both nodes D and E can decode the NAV specified in RTS and CTS correctly, so they defer transmitting their frames during NAV interval(Phase I and II, III). However, since node C and node F are in sensing zone, they can not decode NAV field in RTS and CTS frame. In such case where a node senses a signal but can not decode it, IEEE 802.11 specifies that the node set NAV for EIFS(Extended Inter-Frame Space). So node C and node F set NAV after sensing respective signals(Phase I and II). After that, their behavior and the aftermath differ. Now node A starts transmitting a DATA frame, which can be sensed by node C, but not by node F(Phase III). For node C, this sensing happens before NAV expires, so it defers its frame transmission again. As a result, node C waits until a frame transmission from A to B ends. However, for node F, after NAV expires, it can not sense any signal at all, so it finds the medium idle and proceeds to the operation to send a DATA frame, i.e. switches to its state to contention mode. If it tries to transmit a frame, then a collision should occur(Phase III).

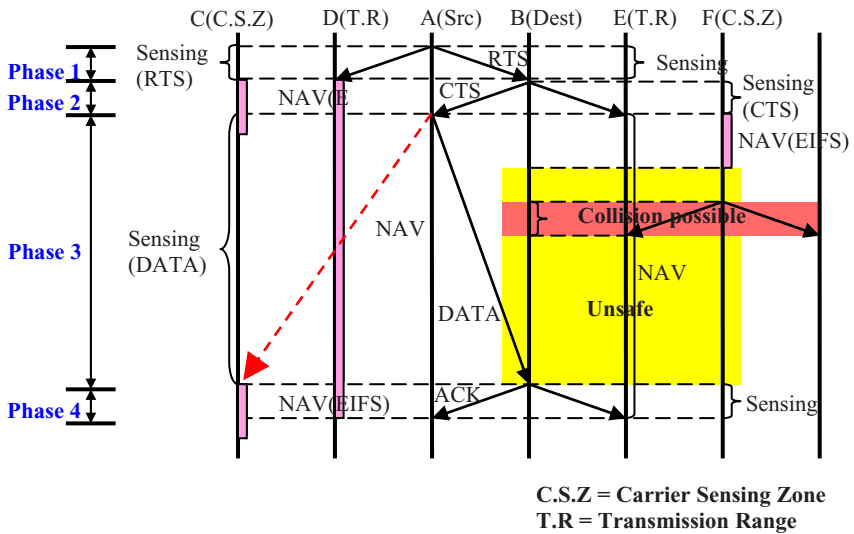


Fig. 2. Collision due to short NAV(EIFS)

As shown in Phase III(Fig. 2), when node F tries to transmit a frame after EIFS, then collision with node B always occurs, which results in discarding the DATA frame that node B is receiving. Once collision occurs for a DATA frame, the sender (node A) will increase contention window and execute the binary backoff process of data link layer and then tries to transmit that frame again. Contention window starts from $32 \cdot aSlotTime[1]$, and the next contention window size is $64 \cdot aSlotTime$, and so on, therefore, the next retransmission will happen during the interval of $[0, 1280\mu s]$, which is still too short for a successful frame transmission. Considering wireless networks where the end-to-end performance is inherently poor and where transmitting in half-duplex mode is one of generic properties, a frame loss due to collision greatly

affects not only performance but also energy efficiency in negative way. In addition, if the lost frame is for a TCP connection, it results in packet loss. This, in turn, will increase the size of the contention window of TCP layer and the binary backoff mechanism of TCP layer will be executed at the source node. These sequences of TCP will negatively affect the end-to-end performance as well, and it is obvious that the consequence will become worse as the number of connections and the capacity of the transmission increases.

One possible solution is to increase the value of $aSlotTime$ such that the contention window size is set to a larger value than the transmission time between the two nodes[3][13]. However, considering the property of ad-hoc networks where nodes can move any time so the topology always changes, it is not an ultimate solution. And also, even in fixed ad-hoc wireless networks, the relative role of a node continuously changes. For example, in Fig. 1, the role of the sender and the receiver changes if the direction of a flow of a connection changes, for example, in bi-directional connections.

From these reasons, protocol behavior should be different for a node in transmission range and in carrier sensing zone.

4 Protocol Improvements

We first make one assumption for protocol improvements that the nodes in carrier sensing zone can know the types of a frame. Even though this assumption might be arguable, because the nodes in sensing zone can not decode signal correctly from the definition(Fig. 1), there are a good solution for assumption. To know the types of a frame which is received in carrier sensing zone, we use multi-channel scheme. Specifically, the IEEE 802.11 in ad hoc mode, the most popular MAC protocol in mobile ad hoc networks, is extended from single channel to multiple channels operation[14]. The current standard allows the practical use of three channels in 802.11b and eight in 802.11a, but multiple channels operation is not supported in ad hoc mode.

A. Transmission on Multi-channel

Among the channels that are able to be used simultaneously, channel 0 is reserved for RTS and CTS frame, channel 1 is reserved for DATA frame, and channel 2 is reserved for ACK frame. Fig 3 shows the frame exchange between sender and receiver on multi-channel.

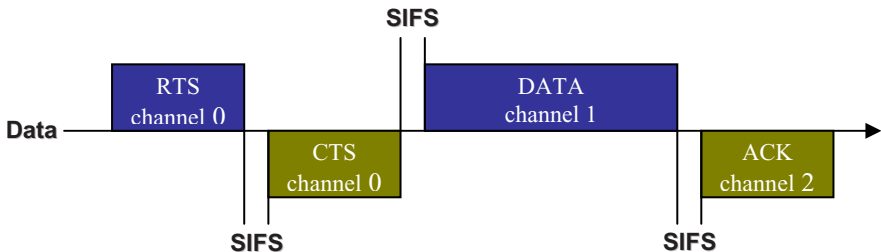


Fig. 3. Frame exchange between sender and receiver on multi-channel

Using multi-channel, nodes in carrier sensing zone can recognize the types of a frame exactly.

B. CAI (Collision Avoidance Interval)

Now we describe our MAC protocol improvements in detail. We first define a term CAI (Collision Avoidance Interval). CAI is defined for a node in carrier sensing zone and is defined as a time interval from the moment when the node in carrier sensing zone senses CTS signal in channel 0 until the node senses ACK signal in channel 2. Therefore, it is time interval necessary for exchanging DATA and ACK frame between a transmitting node and a receiving node. From the motivation in the previous section, NAV, which is set to EIFS in IEEE 802.11, is too short for collision to be prevented, so we use CAI instead of NAV. While CAI, the node defers transmitting a frame, like in NAV, even when the node has a frame to send. But there are two important differences in the protocol behavior. The first difference is that the node resets to CAI whenever it senses another CTS signal while in carrier sensing zone, so it can be repeatedly set to CAI. The reason for this is because of ad-hoc networking property-nodes can move anytime, so the relative location and the role of a node continuously changes. Even in fixed ad-hoc wireless networks, signals can be received from any direction. The second difference is that the node in CAI can answer to RTS frame from other nodes. The reason for this is to improve performance if the node moves out from the carrier sensing zone.

Because of the node mobility, the node which received CTS signal and started CAI can not receive ACK signal. Therefore, it is necessary to define the minimum length of CAI. In 802.11 specification, there are two parameters related to DATA frame size, RTS threshold and Fragmentation threshold. If a DATA frame size is upper the RTS threshold, RTS-CTS is used. If a DATA frame size is upper the Fragmentation threshold, a frame is transmitted using fragmentation. Therefore, the size of all transmitting DATA frame using RTS-CTS is under the Fragmentation threshold. We define the length of CAI, $CAI_threshold$ as follows.

- $txtime(x)$ = transmission time for the frame x
- $CAI_threshold$ = Fragmentation threshold + SIFS + $txtime(ACK)$

From the above description on the modification, the cost for the misinterpretation of frame type is a waste of CAI only. In Fig. 4, the procedure for MAC protocol improvements is presented and commented. Notice that the value of CAI is automatically tuned to the length of current data frame. Fig. 5 shows how collision is prevented by CAI and the new procedure. Comparing to Fig. 2, the unnecessary collision by node F is prevented.

Fairness for the probability of a frame being transmitted is important in ad-hoc wireless networks. In the 802.11 specification, after a frame transmission has completed, every node may attempt to transmit a frame in contention mode. The probability of a transmission changes according to the retry count. For example, a node that has retry count 2 has higher probability than a node that has retry count 3. But a node in CAI has less chance than a node in normal state, because the node in CAI defers its transmission. Although being applied by CAI, a node that has retry count 2 has to

| | |
|--|---|
| <pre> /* protocol behavior state when sensing CTS or ACK */ CAIThreshold = FragThreshold + SIFS + txtime(ACK); if (CTS or ACK sensing in channel 0) { if (during backoff) pause backoff_timer; start CAI; CAI_timer start; } else if (ACK sensing channel 2) { stop CAI ; if (is_channel_idle()) { if (backoff_timer_paused) resume backoff_timer; else { wait for EIFS; proceeds to normal operation; } } } </pre> | <pre> else { /* 802.11 basic operation */ if (backoff_timer_paused) resume backoff_timer; else start backoff_timer; } } } /* Function when the CAI_timer expired */ CAI_timer_handler() { if(during CAD){ stop CAI; /*back to the normal operation of 802.11 MAC protocol*/ } } </pre> |
|--|---|

Fig. 4. CAI and the procedure for MAC protocol improvements

have higher probability than a node that has retry count 3. In our simulation, CAI can start only when the retry count is under 3. The reason for this is that the length of CAI for 1Kbytes data frame is 4697us under 2Mbits/s and this length is almost equal to the backoff time for a node in retry count 3.

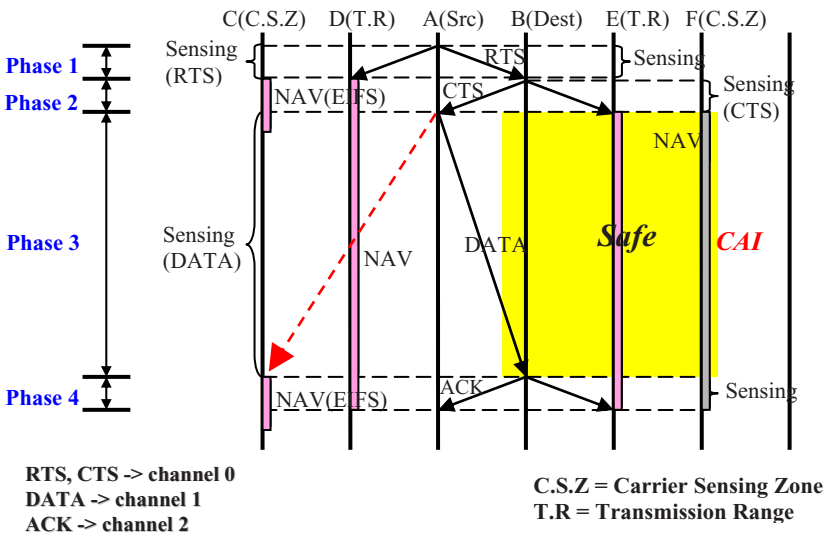


Fig. 5. CAI and Collision prevention

5 Simulation

We have implemented the proposed protocol improvements in *ns-2*[15] and conducted a comprehensive study to evaluate the performance enhancements of 802.11-based multi-hop ad-hoc wireless networks. The main metrics for performance evaluation are end-to-end throughput, the number of collisions, the number of drops and power consumption. We perform simulations for tcp and udp bidirectional connections. The number of connections is 12, the network size is 1000 x 1000(m²), and the number of mobile nodes is 56. *CAI* is set to the length of (Fragmentation Threshold + SIFS + transmission time of ACK frame) to allow one virtual DATA frame transmission. The length of a DATA frame is assumed to be 0.5, 1, 1.5 Kbytes. In order to minimize the interference from a routing protocol, DSDV(Destination Sequenced Distant Vector) routing protocol is used. DSDV[2] is one of the proactive routing protocols and the route update packets are sent periodically and incrementally as topological changes. The performance values are evaluated after running simulations for 300 *ns-2* simulation seconds. The simulations are conducted on Linux 2.4.20 on a Pentium 3.0 Ghz PC with 516Kbytes main memory. The version of *ns-2* is *ns-2.27*.

6 Results

Fig. 6 shows the simulation results of end-to-end throughput for 12 bidirectional tcp and udp connections. Fig. 6 shows that throughputs by our modified protocol always performs better.

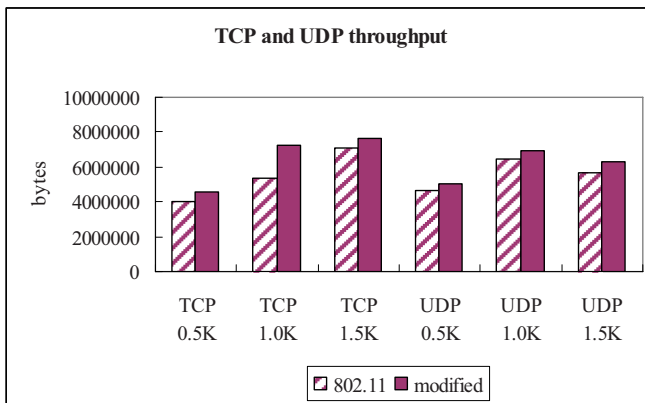


Fig. 6. TCP and UDP throughput evaluation

Fig. 7 shows the comparisons of the number of collisions for both tcp and udp connections. In Fig. 7, the number of collisions represents the number of frame loss at every hop and is significantly reduced as much as 20% for both tcp and udp connections. In fact, this reduction in the number of collisions is the most outstanding feature of our modified protocol.

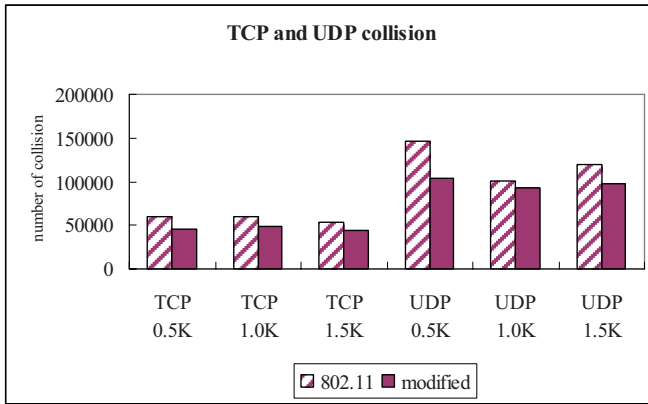


Fig. 7. TCP and UDP collision evaluation

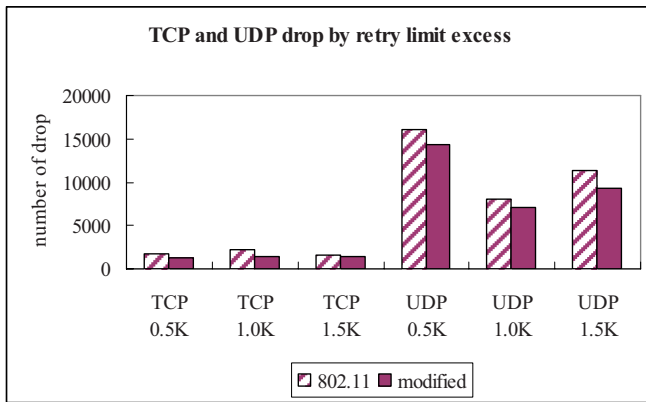


Fig. 8. TCP and UDP drop by limit excess

Fig. 8 shows the comparisons of the number of drops for tcp and udp connections. In 802.11, when a node transmits a frame, it must receive an acknowledgement from the receiver or it will consider the transmission to have failed. Failed transmissions increment the retry counter associated with the frame. If the retry limit is reached, the frame is discarded. In Fig. 8, the number of drops represents the number of discarded frame by retry limit excess at every hop. This number is important in TCP performance, because drop by retry limit excess means end-to-end loss and TCP think this drop as congestion loss. Therefore, to improve TCP end-to-end performance, it is important to reduce the number of drop by retry limit.

Table 1 and 2 show the comparisons of the power consumption for tcp and udp connections. When CAI is applied in a node, the overhead for power consumption is given by 10%, 30%, 50%, 100%. In table 1 and 2, while the total power consumption grows, the power consumption for sending 1Mbytes is reduced.

Table 1. Power consumption for TCP 1.0K traffic

| | 802.11 | O.H 0% | O.H 10% | O.H 30% | O.H 50% | O.H 100% |
|--|-----------|-----------|-----------|-----------|-----------|-----------|
| Idle power consumption | 1855(w) | 1750(w) | 1750(w) | 1750(w) | 1750(w) | 1750(w) |
| Send power consumption | 169(w) | 171(w) | 171(w) | 171(w) | 171(w) | 171(w) |
| Recv power consumption | 2833(w) | 3144(w) | 3144(w) | 3144(w) | 3144(w) | 3144(w) |
| Power consumption by processing overhead | 0(w) | 26.45(w) | 29.10(w) | 34.39(w) | 39.68(w) | 52.91(w) |
| Total power consumption | 4857(w) | 5093(w) | 5096(w) | 5101(w) | 5106(w) | 5119(w) |
| Power consumption for sending 1Mbytes | 0.9297(w) | 0.7210(w) | 0.7215(w) | 0.7222(w) | 0.7229(w) | 0.7247(w) |

Table 2. Power consumption for UDP 1.0K traffic

| | 802.11 | O.H 0% | O.H 10% | O.H 30% | O.H 50% | O.H 100% |
|--|-----------|-----------|-----------|-----------|-----------|-----------|
| Idle power consumption | 1657(w) | 1648(w) | 1648(w) | 1648(w) | 1648(w) | 1648(w) |
| Send power consumption | 217.8(w) | 217.6(w) | 217.6(w) | 217.6(w) | 217.6(w) | 217.6(w) |
| Recv power consumption | 3402(w) | 3430(w) | 3430(w) | 3430(w) | 3430(w) | 3430(w) |
| Power consumption by processing overhead | 0(w) | 14.87(w) | 16.36(w) | 19.33(w) | 22.30(w) | 29.74(w) |
| Total power consumption | 5278(w) | 5311(w) | 5313(w) | 5316(w) | 5319(w) | 5326(w) |
| Power consumption for sending 1Mbytes | 0.8385(w) | 0.6438(w) | 0.8441(w) | 0.8446(w) | 0.8450(w) | 0.8462(w) |

7 Conclusion

In this paper, we addressed the importance of the protocol behavior in carrier sensing zone to prevent unnecessary collisions, and showed that the protocol behavior is required to be modified by in-depth analysis of the protocol behavior. We defined a

term *CAI* to avoid unnecessary collisions and this interval is used for a node in carrier sensing zone instead of NAV when the node senses CTS signal. We conducted a comprehensive simulation study to examine how the performance of the modified protocol in multi-hop wireless ad-hoc networks works. Our improved MAC protocol is completely compatible with the IEEE 802.11 specification, so it can be coexistent with the legendary 802.11-based wireless MAC protocol. With the improvements in the MAC protocol, the number of collisions and the number of drops are decreased as much as 20% and the throughput is as much as 8% for 300 simulation seconds. As a result, we can verify that the end-to-end performance is significantly improved by our MAC protocol enhancements.

References

1. IEEE: IEEE Standard for Wireless LAN-Medium Access Control and Physical Layer Specification, IEEE (1997)
2. Perkins, C., Bhagwatt, P.: Highly Dynamic Destination-Sequenced Distance-Vector Routing for Mobile Computers. *Computer Communications Review*, 234–244 (October 1994)
3. Kwon, Y., Fang, Y., Latchman, H.: A novel MAC protocol with fast collision resolution for wireless LANs. In: *IEEE INFOCOM 2003* (2003)
4. Lin, C.R., Liu, C.-Y.: Enhancing the performance of IEEE 802.11 wireless LAN by using a distributed cycle stealing mechanism. In: *IEEE International Workshop on Mobile and Wireless Communications Network 2002*, pp. 564–568 (2002)
5. Bharghavan, V., Demers, A., Shenker, S., Zhang, L.: MACAW: Media Access Protocol for Wireless LAN's. In: *Proceedings of SIGCOMM 1994*, pp. 212–225 (1994)
6. Cali, F., Conti, M., Gregori, E.: IEEE 802.11 protocol design and performance evaluation of an adaptive backoff mechanism. *IEEE Journal of Selected Areas in Communications* 18(9) (2000)
7. Monks, J.P., Bharghava, V., Hwu, W.-M.W.: A Power Controlled Multiple Access Protocol for Wireless Packet Networks. In: *IEEE INFOCOM 2001* (2001)
8. Acharya, A., Misra, A., Bansal, S.: A Label-Switching Packet Forwarding Architecture for Multi-hop Wireless LANs. In: *ACM WowMom* (2002)
9. Bharghavan, V.: Performance Evaluation of Algorithms for Wireless Medium Access. In: *Proceedings of IEEE International Computer Performance and Dependability Symposium* (1998)
10. Jung, E.-S., Vaidya, N.H.: An energy efficient MAC protocol for wireless LANs. In: *IEEE INFOCOM 2002* (2002)
11. Fujii, T., Takahashi, T., Bandai, T., Udagawa, T., Sasase, T.: An efficient MAC protocol in wireless ad-hoc networks with heterogeneous power nodes. *Wireless Personal Multimedia Communications* (2002)
12. Dutkiewicz, E.: Impact of transmit range on throughput performance in mobile ad hoc networks. *IEEE ICC 2001* (2001)
13. Vitsas, V.: Throughput Analysis of Linear Backoff Scheme in Wireless LANs. *IEE Electronics Letters* 39(1), 99–100 (2003)
14. Choi, N., Seok, Y., Choj, Y.: Multi-channel MAC protocol for mobile ad hoc networks. In: *Vehicular Technology Conference, VTC 2003-Fall 2003 IEEE 58th*, vol. 2 (October 6-9, 2003)
15. <http://www.cisco.com>
16. <http://www.isi.edu/nsnam/ns/>

An Intelligent Event-Driven Interface Agent for Interactive Digital Contents in Ubiquitous Environments

Sukhoon Kang¹ and Seokhoon Bae²

¹ Department of Computer Engineering, Daejeon University
96-3 Yongun-Dong, Dong-Gu, Daejeon, Korea 300-716
shkang@dju.ac.kr

² INUS Technology, Inc.
601-20 Yuksam-dong, Kangnam-ku, Seoul, Korea 135-080

Abstract. Interactive digital contents in the field of networked media and ubiquitous computing enable the consumers to test the features of the product from their handheld computers as if they were using it in real life, by simulating the actions and responses of the product. This new type of digital content can be used extensively to make sales personnel training manuals, sales tools, user manuals and user trouble shooting documents. In this paper, we present the enhanced characteristics of the event flow chart with which the events in an intelligent event-driven interface agent for interactive digital contents in ubiquitous environments, named PlayMo-based agent, are structured. A tree structure can be formed from the array of options or functions. PlayMo-based agent generates the events and gives action commands according to this tree structure, allowing user to perfectly simulate the features and functions of a product simply and directly. The solution to provide intelligent interaction between human and digital contents makes it possible to recreate digital contents by bringing interactivity and intelligence into it.

1 Introduction

What is an ‘interactive digital content’? Simply put, it is digital content that enables the consumers to test the features of the product from their PCs as if they were using it in real life, by simulating the actions and responses of the product. Take the case of an interactive digital content for a mobile phone for example. The user will be able to open the flip panel of the mobile phone by clicking on it. Furthermore, the user will be able to see the numbers being displayed on the mobile phone screen when he/she clicks on the number pad of the phone in the catalog. In other words, an interactive digital content can simulate hundreds of different features to match the features of the real mobile phone to perfection.

An event-driven modeling for interactive digital content, named PlayMo [1, 2, 3], enables the authoring of new digital contents to simulate real world products such as cellular phones, various electronics, machinery and systems on PC. PlayMo-based agent’s independently developed engine, which increases the fidelity of the interactive contents dramatically, provides professional approach in creating layered events and

actions in a visual environment, permitting novice to develop contents without coding or programming. The resulting contents could be compressed into less than a hundred kilobytes for uploading on the web. Also, compared to conventionally available expensive and complicated professional graphic and simulation programs, the PlayMo-based agent provides an inexpensive solution, which allows anyone to create interactive contents easily.

Interactive digital content by using the PlayMo-based agent makes easy, simple and effective design for e-learning, e-catalogue, e-marketing/sales, e-prototyping, customer support, etc. Through its application-ready 3D function visualization solution, engineers and designers can rapidly turn a CAD design model into a 3D interactive virtual product, and the effective function prototyping job can be also completed within a minute.

2 Why Intelligent Event-Driven Interface Agent

PlayMo offers a unique and intuitive modeling method, which received a patent for 'Visual Event Driven, Free Coding Modeling Method'[1] and continuously has refined with collaborative research of academy [2, 3]. PlayMo itself is a powerful developing environment that allows the creation of highly interactive rich media content from a wide range of source files such as still images, video clips, audio clips, 3D models (VRML), CAD models and more. PlayMo's intuitive WYSIWYG editing functions make it easy to embed complex interactivity into models to accurately recreate the functionality of real-world objects, requiring no coding. Publishing electronic products, mechanical components, and dynamic multimedia contents with PlayMo allows users to interact with objects on the internet as if they were real. It is easy to create computer-based training or online/offline education materials based on PlayMo models, and user manuals based on published models for complicated products can be created automatically. PlayMo's content, delivered online or offline, offers enticing product experiences, intuitive web-manuals, effective learning tools, and impressive presentations. The solution, PlayMo-based agent, with the goal to 'provide intelligent interaction between human and digital contents' makes it possible to recreate digital contents by bringing life and intelligence into it in ubiquitous computing environments.

2.1 Notion of Event-Driven Object with Event Flow Chart

Event is an occurrence, which could trigger a change or reaction in PlayMo-powered contents. In other words, event defines user action, which cause specific change or action on the object. These events are assigned to each event node, and event nodes are interrelated with each other in a hierarchy.

PlayMo-based agent enables users to create intelligent 3D contents which react upon various inputs according to the predefined rules of external and internal conditions. The internal structure of this event-driven development environment is made of three independent concepts. The three axes, which constitute PlayMo-based agent are *Object*, *Event*, and *Action*. Object refers to a material such as pictures,

multi-media and text which forms the PlayMo-based agent contents externally. Event refers to an occurrence which could alter or trigger a reaction on interactive digital contents. Action is a result or alteration of interactive digital contents when the predefined event satisfying the condition occurs. PlayMo-powered contents could be defined as organically combined contents which react intelligently to dynamic user inputs.

For example, assume operating an actual cellular phone. It has an appearance of a cell phone as well as its flip, folder, function buttons, sound, LCD screens are its components. PlayMo-based agent handles these as images, GIF Animations, A/V clips and Sound files. These are defined as Objects, the external factors. Next, a user would open the flip or folder on the phone and would press many different buttons. Then, the flip or folder would open, and the LCD display would change with the appropriate sound. In that case, we may define the action opening the flip and pressing the button as external Event being applied to the phone. With these events applied, the cell phone’s flip or folder would open, with the buttons pressed, sounds or display will change. These are defined as Action.

More specifically, PlayMo-based agent generates contents identical to actual product, or intriguing contents possible in the virtual world by creating Objects necessary in the product, and assigning Events such as a mouse click, keyboard input, timer pulse signals, and with an appropriate event, executes variety of Actions possible in the actual item. In PlayMo-based agent, we can organize all the events in a visual event tree using the Event Flow Chart technique. Compared with the traditional State Chart [4] technique, the Event Flow Chart, which controls the events according to the order of precedence and hierarchy, defines events more concretely, explicitly and intuitively. An ‘event tree’ is the hierarchy of functions or the order of interconnected event nodes. Fig. 1 shows this tree structure of events. Events are activated from the ‘root’ and there are three kinds of events in order of precedence: *parent event*, *sibling event* and *child event*.

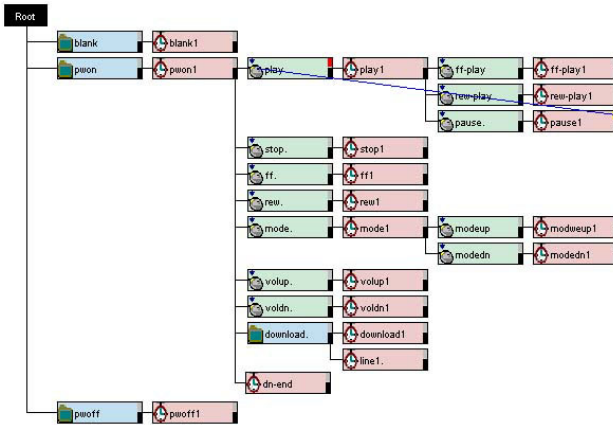


Fig. 1. An Event-driven Modeling Diagram for PlayMo-based Agent

In order to complement control flow more perfectly, we enhanced the Event Flow Chart by extending two characteristics of it:

- (1) **Unconditional Flow:** An unconditional flow proceeds compulsorily. All events, except the events linked with unconditional flow, are ignored during an unconditional flow. This simplifies the Event Flow Chart by avoiding repetition.
- (2) **Synchronous Flow and Return Flow:** Global stack is used for storing the states. When a synchronous event occurs, the current state is pushed into the stack. On the contrary, states in the stack will be popped up when a return event occurs. A synchronous event, as an interrupting event, is needed for the system to return to the original state.

Rules of governing flow are as follows. Going from one event location to the next event, there is an event that should be executed and an event that should not be executed. In other words, it cannot be executed a close command when the lid hasn't even been opened. From these laws of physics, PlayMo-based agent gives a few rules governing the flow of events:

- [Rule 1]: May flow to an event node that is one step below as shown in Fig. 2.
- [Rule 2]: May flow to event nodes on the same level as shown in Fig. 3.
- [Rule 3]: May flow to an event node that is many steps above.
- [Rule 4]: May not flow to an event node located more than two steps below as shown in Fig. 4.
- [Rule 5]: May not flow from an equal level or higher level event node to a lower level event node on a different branch as shown in Fig. 5.

Let's explore first of all, the relevant event node from the child node of a currently activated event node.

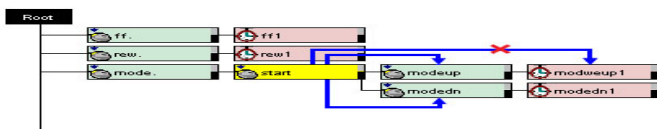


Fig. 2. [Rule 1]: May flow to an event node that is one step below

If nothing is found from the above search, explore sibling nodes connected to the same parent node.

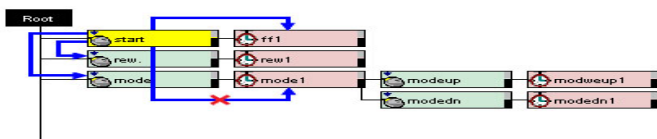


Fig. 3. [Rule 2, 3]: May flow to event nodes on the same level and to an event node that is many steps above

Search other levels of parents from the activated node, or its siblings. This only connects to the direct branch connected to the Root. In other words, you cannot go from a sibling parent that is not its direct parent to its offsprings.

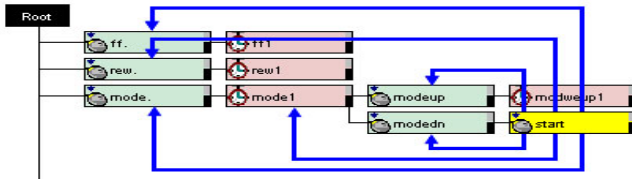


Fig. 4. [Rule 4]: May not flow to an event node located more than two steps below

There may be areas where the above rules cannot be used to connect, but a connection is necessary nevertheless. We use the Goto Line in these instances. Drag from the box located on the top right hand corner of the activated event node to the event node to be connected. This creates a blue line. This will move the flow to the Goto Line connected point, immediately when the flow reaches the activated event node. At this time, check GotoEventWithAction from the even panel options. As it is being moved, it will execute the action included in the event node that is located in the position it is being moved to. When you check the next GotoEventWithoutAction, it moves without executing the action in the event node.

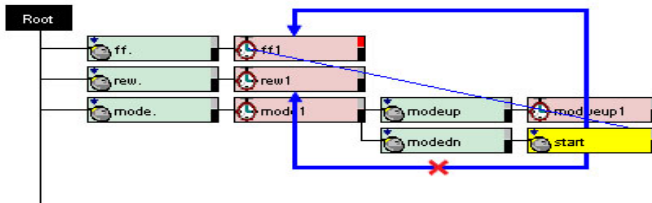


Fig. 5. [Rule 5]: May not flow from an equal level or higher level event node to a lower level event node on a different branch

2.2 Seamless Integration in Ubiquitous Computing Environments

It is reasonable to define ubiquitous computing as the attempt to break the pattern paradigm of the traditional relationships between users and computational services by extending the computational interface into the user's environment [5]. Given the large numbers of devices and services that users will encounter in ubiquitous computing environments, there are many situations that will require that users serendipitously compose available resources into configurations suitable for their current activities. A scalable interface to interactive digital contents would provide a unified service with multiple device interfaces. The challenge in this case is to provide free-coding capability to enable radically different interaction methods with the same underlying data and service. An intelligent event-driven interface agent for interactive digital

contents in ubiquitous environments is only one part of what we call a ubiquitous software service, a service that actively searches out the user at convenient and salient times. Users interact with a variety of services and there are some obvious connections between the information that each service manipulates. Furthermore, this set of services is constantly subject to change. How can we provide intelligent ways to integrate the behavior of these different services without requiring additional programming effort by both the designer of a service and the end user? With intelligent event-driven interface agent, developers and end-users will better understand a concept via rich media representation. By way of designing an intelligent event-driven interface agent, the look-and-feel aspect will provide a life-like image immediately. PlayMo itself is designed by way of a user-friendly approach without coding. As such, the trouble of programming and algorithms are unnecessary: Simply, click, label, paste, and scroll.

2.3 Comparison with Other Works

Behavior representation models are classified as event model and state model. In event model, object action is constant in response to an event. Therefore, the characteristics of easy-to-learn and intuitive event flow design are definitely strong points, and exponentially increasing complexity, e.g., Web3D (Viewpoint, Cult3D, etc.), is weak point.

In state model, object action is varying according to its state in response to an event. Therefore, effectiveness to represent highly complex action relations seems to be strong point. The characteristics of hard-to-learn and initial design, e.g., system development tools (Rapid+, ROSE, OpenGL) are weak points.

Our interface agent model has the following characteristics of state and event conjugated model:

1. State-of-the-art concept to take full advantage of each model.
2. Automated state model conversion from designed hierarchical event tree.
3. Minimizing authoring cost while maximizing operation reality.
4. The most effective way to represent complicated operation relations.

Visual representation quality or richness of all kinds of simulation object such as bitmap image, movie clip, 3D model, sound clip, etc are the important factors. In case of 3D model, texture mapped rendering quality is the most crucial factor.

Regarding level of interactivity, in lowest level, sequential simulation is based on limited number of pre-defined scenarios. In highest level, arbitrary simulation is in response to user's random input (event).

Operational reality is the ratio of actual model's number of actions (functions) to simulation model's. Perfect operation reality is not always required to achieve a simulation purpose.

Regarding application-specific features, simulation system's capability to support application specific functionalities can be operation history logging, printable document generation, etc. It makes a direct effect on overall authoring cost.

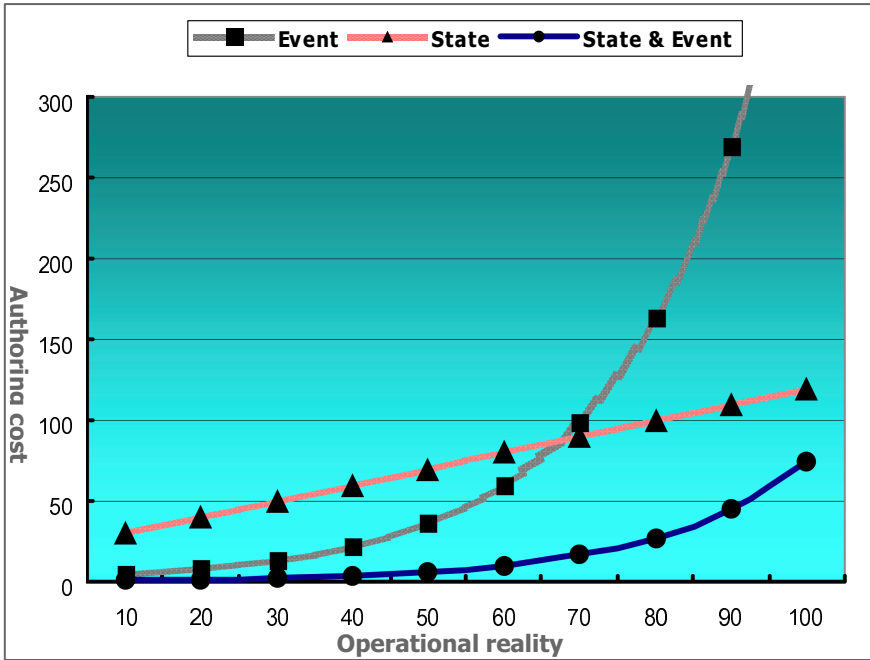


Fig. 6. Operation reality in behavior representation models

Table 1 shows that our interface agent model offers better solutions than similar models in the following fields.

Table 1. Comparison with other tools

| Level 1 (no-interactivity) | Level 2 (simple triggering) | Level 3 (low-interactivity) | Level 4 (high-interactivity) |
|--|---|---|--|
| <p>Single action time-line control</p> | <p>Multiple actions unconditional play & stop control</p> | <p>Multiple actions Non-systematic & conditional play & stop control</p> | <p>Multiple actions Systematic & conditional play & stop control</p> |
| <p>User controls only playing or stopping a set of sequentially defined actions in a certain time-frame.</p> | <p>Multiple sets of actions are defined and user triggers one or more actions independently. No relations are supported between multiple actions.</p> | <p>Multiple sets of actions are related with each other under the user defined rules described in script or program code. However, simulation engine itself does not support such relations systematically.</p> | <p>Multiple sets of actions are related with each other under the simulation engine based on vendor's own methodology.</p> |
| <p>Animation</p> | <p>Viewpoint PowerPoint Cult3D Flash</p> | | <p>PlayMo Rapid+</p> |

3 Work Flow in Intelligent Event-Driven Interface Agent

A brief description of the process for interactive digital contents involved in working with *PlayMo based agent* is as follows.

- Step 1 (Analysis for Product Function):** Function to analyze is concrete action such as button. It would be better imagine the structure of a product and consider each reaction of each event in right or wrong action.
- Step 2 (Preparatory to Image Source):** It is necessary to get image source of product to design include sounds and motion images. Crop the image into object images to each function then save them.
- Step 3 (Object Import and Property Set Up):** Create new project and import saved image source in OBJECT mode. Arrange each image at proper position. Create other multimedia sources such as html, motion images, sound, timer and the like. Then, set up the property type to each object.
- Step 4 (Creation of Events):** Create events on each image source depend on user command like mouse click, over, keyboard hit and so on.
- Step 5 (Creation of Action):** It is necessary to create action on each event. An action means real interactivity such as 'show or hide of object' and 'play on and off music'.
- Step 6 (Arrangement of an Event Tree):** Event has the order system as we can play music after turn on the power. This order structure is almost similar to that of real product. A button could do another action at certain situation, however, it could be treated all the complete problems related the function structure with event tree.
- Step 7 (Simulation):** It is possible to see the interactive digital contents like real products with simulator.
- Step 8 (Debugging):** Start debugger, it is possible to see which event is acted at real time and also see list of action activated on output window. With Debugging tool and Watch Window, it is possible to check out special action that users want. After go through these kind of whole things, users could get perfect product simulation.

4 Implementation of Intelligent Event-Driven Interface

One of the main interface functions in PlayMo-based agent for interactive digital contents is as follows.

1 Title Bar: Default title bar displayed when PlayMo is launched.

2 Menu Bar: When PlayMo is opened initially, menus are listed in the order of File, View, Tools, Help. As the picture displayed above, when a new content is being created, or existing contents file is opened(.at3), the menu will appear in the order of File, Edit, View, Object, Event, Debug, Tools, Window and Help.

3 Icon Bar Set: Icon Bar Set is a set of icons including a series of commands frequently used in the menu to provide assistance. Title of the icon is displayed when the mouse pointer is on top of the icon. Icon will change into pressed form when clicked.

- 4 Project Tab:** Displays name of the project and may change work area.
- 5 Object Window:** Window aligning Objects such as 3D image of the target product, A/V files according to the aim of the user. The Object panel is used to open a file.
- 6 Event Window:** Window creating an Event node to assign Event and Action command to the opened 3D Object. Event node identical to the picture above is created and interconnected. Event and Action commands are executed in each event and action panel.
- 7 Panel:** On the Panel, users can define the attributes of active objects and event nodes. The Panel is divided into Object, Material, Event and Action panel. When each panel is selected with the mouse, that particular panel is activated enabling the user to define the attributes of each of them.
- 8 Status:** Shows the current status of PlayMo. Located on the bottom of the GUI.

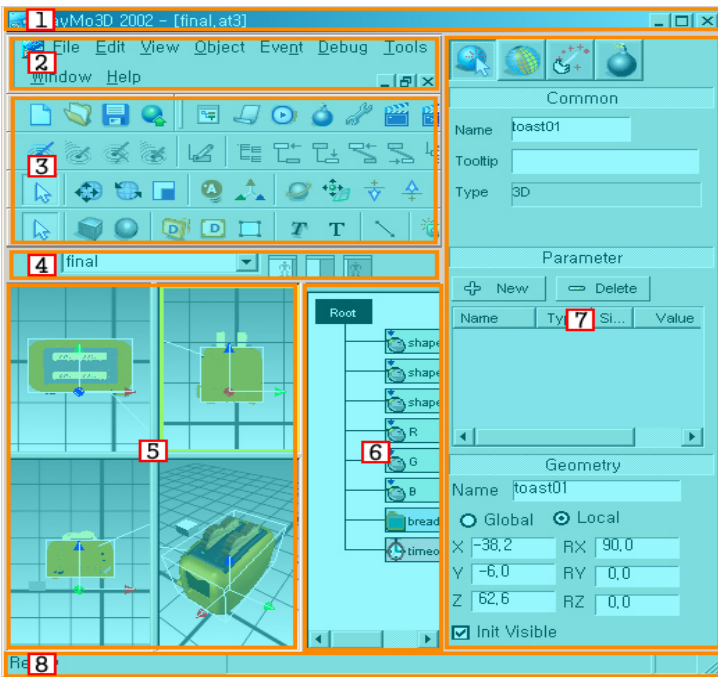


Fig. 7. Example of Intelligent User Interface for PlayMo-based Agent

5 Conclusions

Ubiquitous computing focuses on user interaction in real operating environments. Both ubiquitous computing and interactive digital contents are strongly linked together. We think one important point in ubiquitous computing is that the devices provide smart support to user without forcing the user to change behavior. The access to devices should not be complicated due to the fact that they offer more functionality. Often the opposite is the case - the devices become too complex and people just use

the very basic functions. We emphasize that the way people will interact with their environment is not changed in general.

Intelligent event-driven interface agent is dedicated to deliver smart and simple environments to enrich the contents on websites, education, advertising, or industrial design and modeling. By way of designing an intelligent event-driven interface agent, the look-and-feel aspect will provide a life-like image immediately. PlayMo itself is designed by way of a user-friendly approach without coding. As such, the trouble of programming and algorithms are unnecessary. Simply, click, label, paste, and scroll.

Content powered by intelligent event-driven interface agent improves management decisions, perks marketing content, simplifies training materials, and intensifies learning resources. All data is digital, and can be retrieved and stored anywhere at anytime.

Integrating intelligent event-driven interface agent with product data management, customer relationship management, supply chain management or other IT technologies in terms of product or component realistic visualization, fully integrative function simulation and real time product customization etc., users can get the priceless value and take advantage of using the virtual work environment on products through internet or mobile platform over the whole life cycle of the product. It is important to note the fact that our interface agents can will be deployed in real applications in the short term because they are simple, operate in limited domains and do not require cooperation with other agents.

References

1. INUS Technology, Inc., Visual Event Driven, Free Coding Modeling Method, Patent (2001), <http://www.playmo.com>
2. Kang, S., Hur, C.J.: PlayMo: An Event-Driven Modeling Tool for Active Catalog. In: Proceedings of 29th EUROMICRO Conference, Belek, Turkey (2003)
3. Kang, S., Bae, S., Hur, C.J.: A Development Environment for Interactive Digital Contents: PlayMo3D. In: Proceedings of 30th EUROMICRO Conference, Rennes, France (2004)
4. Harel, D.: STATEMATE: A Working Environment for Development of Complex Reactive System. *IEEE Transaction on Software Engineering*, 403–414 (1997)
5. Lindenberg, J., et al.: Improving Service Matching and Selection in Ubiquitous Computing Environments: A User Study. *Personal and Ubiquitous Computing*, 59–68 (2007)

A Loop-Based Key Management Scheme for Wireless Sensor Networks

YingZhi Zeng¹, BaoKang Zhao^{1,2}, JinShu Su¹, Xia Yan^{1,3}, and Zili Shao²

¹ School of computer, National University of Defense Technology, ChangSha Hunan, China

² Department of Computing, The Hong Kong polytechnic University, Hong Kong

³ School of Computer and Communication, Hu'nan University, ChangSha Hunan, China

zyz1234@gmail.com, sjs@nudt.edu.cn,

sunofxy@hotmail.com, {csbzhao, cszlishao}@comp.polyu.edu.hk

Abstract. Wireless sensor networks are emerging as a promising solution for various types of futuristic applications for both military and the public. The design of key management schemes is one of the most important aspects and basic research field of secure wireless sensor networks. Efficient key management could guarantee authenticity and confidentiality of the data exchanged among the nodes in the network. In this paper, we propose a new key management scheme based on loop topology. Comparing with cluster-based key management schemes, loop-based scheme is proved to be more efficient, cost-saving and safe.

1 Introduction

Recent advancements in wireless communications and micro electromechanical technologies have promoted the development and applications of wireless sensor networks (WSN). WSN increasingly become viable solutions to many challenging problems for both military and the public applications, including battlefield surveillance, border control, target tracking and infrastructure protection.

In a WSN, sensor nodes are typically deployed in adversarial environments such as military applications where a large number of sensors may be dropped from airplanes. Sensor nodes need to communicate with each other for data processing and routing. Secure communication between a pair of sensor nodes requires authentication, privacy and integrity. However, the wireless connectivity, the absence of physical protection, the close interaction between sensor nodes and their physical environment, and the unattended deployment of sensor nodes make them highly vulnerable to node capture as well as a wide range of network-level attacks. Moreover, the constrained energy, memory, and computational capabilities of the employed sensor nodes limit the adoption of security solutions designed for traditional networks.

As a successful security mechanism of wired networks, key management is crucial to the secure operation of sensor networks. A large number of keys need to be managed in order to encrypt and authenticate all sensitive data exchanged. The characteristics of sensor nodes and WSNs render most existing key management solutions developed for other networks infeasible. To provide security in such a distribution environment, the

well-developed public key cryptographic methods have been considered at first, but these demand excessive computation and storage from the resource extra-limited sensor nodes [1]. The symmetric key cryptography is considered as the only feasible way for wireless sensor networks. Therefore, there must be a secret key shared between a pair of communicating sensor nodes. Sensor nodes can use pre-distributed keys directly, or use keying materials to dynamically generate pair-wise keys.

Since the network topology is unknown prior to deployment, a key pre-distribution scheme is required where keys are stored in ROMs of sensor nodes before the deployment. The stored keys must be carefully selected so to increase probability that two neighboring sensor nodes, which are within each other's wireless communication range, have at least one key in common. Those nodes which have no shared keys may setup secure communicate through the help of neighboring nodes. After the deployment, each sensor node should connect with its neighboring nodes and generate their security keys in a self-organized method. After Key generation, next important step is distributing the keys to relative nodes.

The main contribution of this work is to shed some light on the basic framework of the key management scheme of WSN. Loop-based scheme includes key material pre-distribution, key generation, key distribution and rekeying. In particular, we bring in a novel loop-based topology for key management. To the best of our knowledge, this paper is the first one to apply loop topology to key management scheme in distributed wireless sensor networks. Our analysis and comparison indicate that this approach has substantial advantages over the traditional cluster-topology scheme.

The remainder of the paper is organized as follows. Section 2 provides an overview of the related works. The loop-based key management scheme is introduced in section 3. Section 4 deals with the detailed performance analysis and comparisons. We conclude in Section 5 and point out some future research directions.

2 Related Works

A number of key management schemes have been developed for sensor networks in the recent years. In this section, we review the major existing key management schemes in wireless sensor networks.

Eschenauer and Gligor [2] proposed a random key pre-distribution scheme. Each sensor node is assigned k keys out of a large pool P of keys in the pre-deployment phase. Neighboring nodes may establish a secure link only if they share at least one key, which is provided with a certain probability based on the selection of k and P . A major advantage of this scheme is the exclusion of the base station in key management. However, successive node captures enable the attacker to reveal network keys and use them to attack other nodes. Based on the EG scheme, q -composite keys scheme was proposed by Chan in [3]. The difference between this scheme and the EG scheme is that q common keys ($q > 1$), instead of just a single one, are needed to establish secure communication between a pair of nodes. Using the framework of pre-distributing a random set of keys to each node, Chan presented two other mechanisms for key management. The first mechanism is a multi-path key reinforcement scheme, applied in conjunction with the basic scheme to yield improved resilience against node capture attacks. The main attractive feature of this scheme is that it can enhance the security of an established link key by establishing

the link key through multiple paths. The second mechanism is a random pair-wise keys scheme. The purpose of this scheme is to allow node-to-node authentication between communicating nodes.

Liu and Ning [4] provided further enhancement by using t -degree bivariate key polynomials. Since an attacker needs to capture at least $t+1$ nodes to obtain any t -degree polynomial, this solution was shown to significantly enhance network resilience to node capture as long as the number of captured nodes is below a certain threshold. However, if the number of captured nodes exceeds this threshold, the network is almost entirely captured by the attacker.

Du et al. [5] proposed a method to improve the basic scheme by exploiting a priori deployment knowledge. They also proposed a pair-wise key pre-distribution scheme for wireless sensor networks [6], which uses Blom's key generation scheme [7] and basic scheme as the building blocks.

Choi and Youn [8] proposed a key pre-distribution scheme guaranteeing that any pair of nodes can find a common secret key between themselves by using the keys assigned by LU decomposition of a symmetric matrix of a pool of keys.

3 Loop-Based Key Management Scheme

Existing approaches in key management scheme mainly inefficiently utilize the cluster topology information. In fact, the loop-based topology has many special benefits in WSN. We present a new key management scheme based on the loop topology. To our knowledge, this is the first paper in this area that combines the node topology with key management.

3.1 Basic Definitions

In Graph Theory, a loop is a non-directional path, which begins and ends with the same node. Since there is at most one connection between every two nodes in an undirected graph $G=(V, E)$ [9], a path from v_i to v_j representing a wireless sensor network link can be defined as a sequence of vertices $\{v_i, v_{i+1}, \dots, v_j\}$, where V representing the set of nodes and E is the set of connections.

Loop length: The length of a loop also can be called path length, is the number of hops from v_i to v_j . Let L be a loop. It is obviously that if $\text{length}(L) < 3$, either the node on L is isolated or L is a round trip between two nodes.

Loop type: In a large scale WSN, there may be some isolated nodes. A loop with only two nodes is also a special loop. For example, in Fig.1, L_2 and L_3 are typical loops and L_1 is a two-nodes special loop. In the following parts, nodes on the loops with greater length than 2 are called on-loop nodes. Let L be the set of the loops that node v is on. If $\max(\text{len}(l) \leq 2)$ (for every l in L), we say v is non-on-loop node.

3.2 The Loop-Based Topology

Unlike traditional wired networks, WSN is a data-center network. Its core function is to aggregate data and to forward data through the route nodes to the sink. In our key management scheme, we consider the key management topology and the data process topology should not be separated.

Old key management schemes are mainly based on cluster topology. Under the assumption that a sensor node either acts as a data producer or is just a router, every node should take part in a voting to choose some nodes acting as cluster headers. After the deployment of nodes and the CH's voting, the cluster headers play an important role in the next steps which include initializing keys, distributing group keys and rekeying. There are two kinds of working flows in cluster-based key management schemes. Key management flow is under the control of those cluster headers. Data aggregating flows are processed between nodes doing sensor works.

In this paper we take loop as the basic unit and the entire network is grouped into inter-connected loops in self-organized mode. Within a loop, nodes can exchange information with each other by forwarding messages along the loop in either of the two directions. For inter-loop communications, messages are first routed to the gateways nodes (router nodes joining multiple loops) and transferred from gateway to gateway till reach the destination. As for inner Loop transmission, messages are finally forwarded to the destination.

Loop topology has many special benefits in WSN:

(1) The loop topology is relative to the physical positions of those nodes directly. When a node within the loop receives an order to sense some special information, the node becomes an information aggregator immediately. Every neighboring node gets some sensor data and sends it to the aggregator. The aggregator will compare and integrate it with its own report. The result would be shortened before it is sent to the next hop. Hop by hop, the sensor data will be shortened and be aggregated many times until it arrives at the sink node. (2) There are no critical header nodes defined in a loop, so the network topology never suffers from chain change caused by the re-election of headers. The scenario of a group without leader will never happen in a loop-based WSN. (3) Local loop information can be reserved in every node on the loop. The topology information redundancy enhances the network robustness. (4) One of the features of a loop that there are two paths between every two nodes on the same loop provides a backup route for link failure during message transmission.

3.3 Creation of a Loop Topology for Key Management

1、(Key material pre-distribution phase) Before the deployment, every node should be assigned some key materials, including a unique ID, a private key (only known by the key server and node itself), a Hash function and a global key. After deployment, every node will start broadcasting its ID message encrypted by the global key. This action can prevent malice listening during the initialization phase of key management.

2、Every node which receives a message can build up its neighbor table.

3、**Condition 1** for Loop formation: After checking their neighbors' information, those nodes with only one neighbor will start the second round broadcasting, such as node A in Figure-1. The information of their neighbor table (NT) is broadcasted. Neighboring nodes received NT messages will add the neighbor information into their link table (LT) and broadcast the latest LT messages to neighboring nodes.

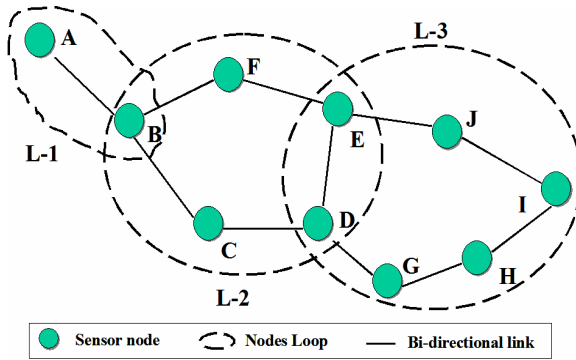


Fig. 1. An example for loop-based wireless sensor networks

If the sensor nodes are deployed close enough then none of them has only one neighbor. **Condition 2** for Loop formation should be taken into consideration. Timing is the first key point. At time T_1 after the deployment, one-neighbor node can start sending message. If none of the nodes has only one neighbor, those nodes with at least M neighbors ($M \geq 3$) can start broadcasting their NT at time $T_1 + nT$ (Unit time T equals to the time a node broadcast would need). If $n=5$ in Figure-1, then node I will start sending its NT message. Table-2 lists those messages (including messages sender, receiver and contents) passed among some nodes in Figure-1. The message processing details and sequence are shown in Table-1 and Figure-2.

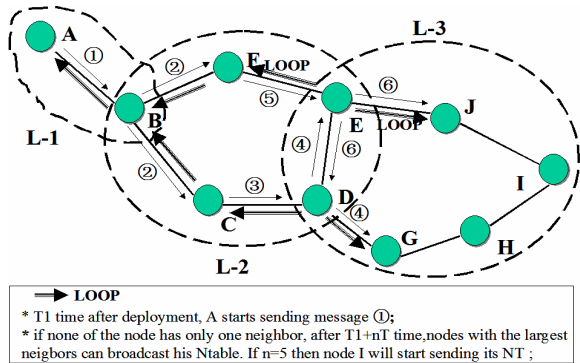


Fig. 2. An example of a loop’s creation

4、Forming loop: After several units of times nT , some nodes, such as B in Figure-1, may receive two loop messages from neighbors. Within the node sequence that a node can find a multiple-hop path to connect itself, a loop of those nodes can be formed by the conjunction of loop messages. Thus the whole sensor networks can be divided into many loops, among them are some special loops. Two loops may share two and even more common nodes, such as L-2 and L-3 in Figure-1.

Table 1. Loop creation Messages

| Node ID | Received Msg | | | Send Msg | | |
|---------|--------------|-------|-------------------|----------|-------|-------------------|
| | ID | from | content | ID | to | content |
| A | | | | ① | B | {} |
| B | ① | A | {} | ② | C,F | {C,F} |
| C | ② | B | {C,F} | ③ | D | {F,B} |
| D | ③ | C | {F,B} | ④ | E,G | {F,B,C} +{E,G} |
| E | ⑤ | F | {C,B} | ⑥ | D,J | {C,B,F} |
| E | ④ | D | {F,B,C} +{E,G} | LOOP | F,J | L-2 {F.....F} |
| D | ⑥ | E | {C,B,F} | LOOP | C,E | L-2 {F.....F} |
| F | LOOP | E | L-2 | LOOP | B | L-2 |
| C | LOOP | D | L-2 | LOOP | B | L-2 |
| | | | | | | |

5、 Special loop format: A single-link node, such as node A in Figure-1, has only one link with a neighbor node. Those two nodes (A and B) form a special loop L-1. Only when a node receive a message {} come from his neighbor node can this kind of special loop be created. Through step 1 to 4, another loop L-3 can be formed by node E, D, G, H, I and J. It is obvious that two nodes (D and E) are shared in loop L-2 and L-3. This type of loop format is determined by the loop size and the node position.

3.4 The Loop-Based Key Management Scheme (LBKMS)

As described in section 3.3, the first stage of LBKMS is to form loops through step 1 to 5. All the nodes of a WSN are divided into different loops or shared between neighbor loops.

Based on the loop topology, this paper develops a new key concept: loop-key. Upon loop information (every node get its neighbor table and link table and loop sequence), the loop-creator node can set up a new loop-key for those nodes in the loop. The computing formula of loop-key is:

$$\text{Loop-key} = \text{Hash}(\text{time stamp} \parallel \text{private key} \parallel \text{loop-creator node ID} \parallel \text{some loop members' ID}). \tag{1}$$

Time stamp is introduced into above formula to prevent replay attack that comes from neighboring nodes. The private key is a proprietary key of loop-creator. It is also the creator’s privilege that how many loop members’ IDs are used in the hash function. For example of Figure-1, the loop-key may be equal to hash (T_s|| K_B|| B|| C|| D|| E).

This formula is based on the preloaded material on each sensor node, using time stamp and other loop nodes’ ID can guarantee the production-loop key be safe.

In the third stage, loop-creator will send the loop-key encrypted with the global key to its loop members through the loop routing. If the loop format is not special, the key messages will be sent to its two loop-neighbors at first. Every node on the loop will send the key message to next node on the neighbor table until some node receives the same message twice.

After the above three stages, every node in WSN should belong to a loop group and should keep a loop-key shared with other loop members. Sensor data aggregation and communication within the loop should be encrypted using the loop key.

The loop-based rekey: Well known as a resource-limited network, a WSN cannot afford changing loop-keys continually. But there are still two scenarios in which rekeying is sometimes needed. In the **first scenario**: If a loop member is recognized as a defection node, or the sink sends a command to clean some node, the urgent affair is to kick it out of the loop member list. First of all, such an abnormal message arrives at the closest loop member. The node will send a cleaning message to its two loop neighboring nodes (if the defection node has just one direct neighbor, then just one cleaning message is enough.). As is shown in Figure-3, cleaning message should be sent to every node on the loop except the defection node. After that, the first leader node will start sending rekeying message to replace the old loop-key.

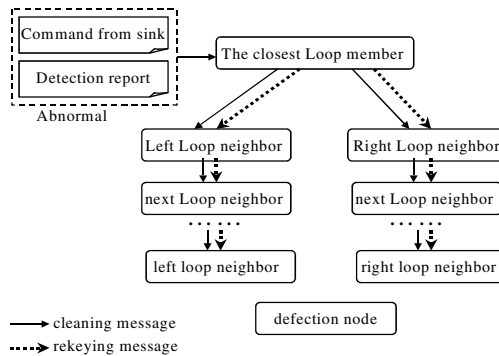


Fig. 3. Loop-based rekeying in WSN (1)

Compared with first scenario, the **second scenario** deals with normal rekeying. If a loop member is out of battery and can-not work properly any more, it should be deleted from the loop list, and the loop-key that it shared with other members should also be abandoned. So the working flow in Figure-4 is to clean old loop-key stored on every loop member. The second step is to set up new loop-key. For the sake of saving rekeying time, the new key’s creator is the loop node that has received the same cleaning messages twice.

In one word, the rekeying process is very important in long-time WSN. Loop-key should be changed as quickly as possible if some defection nodes are found. At the same time, normal key updating is also a good step to keep WSN safety.

Security enhancement in rekeying: Because defection nodes can overhear neighbors’ messages during the rekey process, so some measures should be taken to keep the communication between remain nodes of loop in the overhearing area to be safe. Here we assume that a defection node can only overhear its one-hop neighbors’ messages. It is obviously that we cannot prevent a defection node from hearing the first cleaning message, but we can stop him from getting new keys and other damages may cause by him. For example in Figure-1, if the node I is defected, link E-J and G-H should use new keys which node I cannot compute base on the pre-shared material and overhearing contents.

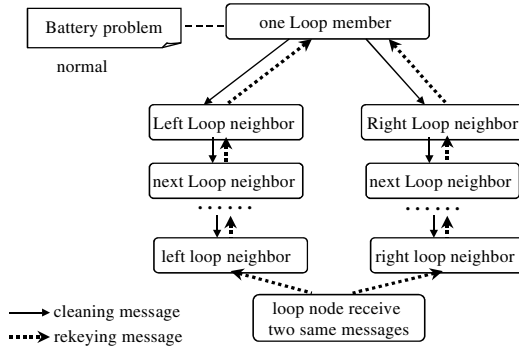


Fig. 4. Loop-based rekeying in WSN (2)

We use the polynomial-based key pre-distribution protocol proposed by Blundo et al. [10] to establish a new key shared between the last cleaning message’s sender and receiver. The new key is only created and used between the sender and receiver, so it is a pair-wise key. Firstly before sensor nodes’ deployment, one key sever

randomly generates a bivariate t-degree polynomial $f(x, y) = \sum_{i,j=0}^t a_{ij}x^i y^j$ over a finite

field F_q , where q is a prime number that is large enough to accommodate a cryptographic key, and has the property of $f(x, y) = f(y, x)$. For each sensor node i with a unique ID, the key server computes a polynomial share of $f(x, y)$, that is, $f(i, y)$. For any two sensor nodes i and j , node i can compute the common key $f(i, j)$ by evaluating $f(i, y)$ at point j , and node j can compute the common key with i by evaluating $f(j, y)$ at i . So to establish a pair-wise key both nodes just need to evaluate the polynomial with the ID of the other node without any key negotiation and the defection nodes know nothing of the new key. The scheme is proved secure and t-collusion resistant in mathematics.

At the same time, we also can use the time stamp to prevent fake cleaning messages made by the defection nodes.

4 Analysis, Simulation and Comparison

Nodes organization is the basic for research of WSN. WSNs of clustered organization are viewed as the most energy-efficient and most long-lived class of sensor networks [11]. There exist some key management schemes for WSN that are based on the cluster topology [12~14].

Creating a cluster for key management in a wireless sensor network at least includes 5 steps. Here we use the max connection degrees method as an example:

1. Similar to our loop-based scheme, every node broadcasts its ID to its neighbor nodes;
2. After received neighbor’s ID message, every node calculates its neighbor numbers and send it with the neighbors’ IDs to the neighbor nodes;
3. A node whose connections is bigger than its neighbors can send a cluster-head-request message to its neighbors;

4. Every node with lower connections sends a reply message to those cluster-head-request messages: join or reject. Nodes that received different request messages have to choose one of those cluster-head campaigners as their cluster header. Which node to be chosen is determined by ID or other parameters.
5. After received enough join messages from neighbor nodes, the cluster-head candidate can set up a cluster key with its cluster members.

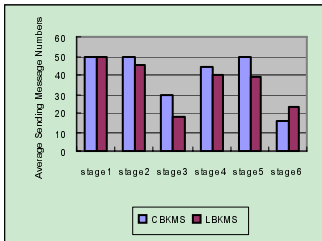
It is obvious that the key management based on cluster topology is more complicated than our scheme described in section 3. According to the comparison in table-2 and 3, the results can be showed as follows:

Communication cost: As a resource-poor network, WSN cannot afford too much communication among its nodes. The cluster-to-cluster relationship is more complex than that of loop-to-loop. It is common that some neighboring nodes are shared between two loops. But it would be redundant that more than one node are shared between two clusters. Two close clusters will cost more energy on the communication than two loops.

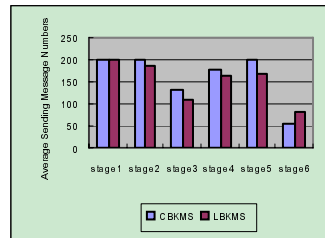
Storage cost: The cluster-based topology has to save neighbor clusters' information as route in the header and some members' storage. On the contrary, in the loop-based topology, the neighbor route information is already broadcasted during the second stage of the loop's forming.

Table 2. Cluster-based VS loop-based in communication

| CBKMS | | | | LBKMS | | | |
|-------|------------------------------|--------------------------|-------|-------|--|------------------------------|----------------|
| stage | action | content | cost | stage | action | content | cost |
| 1 | All nodes broadcast | Self ID | | 1 | All nodes broadcast | Self ID | |
| 2 | All nodes broadcast | Neighbor IDs and numbers | large | 2 | A few nodes broadcast other nodes broadcast | Neighbor table Link table | small small |
| 3 | Some nodes broadcast | Cluster head request | | 3 | those nodes find match Loop link broadcast | LOOP | small |
| 4 | Neighbor nodes of some nodes | Reply message | large | 4 | other nodes broadcast | LOOP | |
| 5 | all nodes broadcast | Cluster inform | | 5 | Some Nodes receive same LOOP messages from two neighbors broadcast | Loop inform | |
| 6 | All headers broadcast | Cluster key | small | 6 | Loop-creator | Loop key | large |



Network size=50 nodes



Network size=200 nodes

Fig. 5. Sending message numbers contrast

Communication is the biggest energy consumer. Especially the cost of sending message is much larger than receiving message. We use ns2 to simulate WSN with different network size and apply CBKMS and LBKMS at same conditions. After calculating average sending messages numbers, the contrast result is list in Figure-5. We can find that CBKMS send more messages than LBKMS from stage1 to 5, only in stage 6 that loop key have to be transmitted more hops than cluster key.

From perspective of security, the loop-based Key management scheme is safer and more stable than the cluster-based one.

Firstly, those two schemes have different role assignment among sensor nodes. The difference is listed in Table-4. From the comparison table we can find that CBKMS assigns many important tasks on cluster headers. A header node will play as a header all the time till it is replaced by another node. A loop creator’s identifier initializes a loop’s forming and has right to generate a loop key. After the loop is formed, there is no difference between normal nodes and the loop creator.

According the probability theory, every member in a loop topology has equal probability to be caught. Once a loop member is lost, its loop-neighbors can set up new loop quickly. What they need to do is to deleting the lost node ID from the loop sequence and generating a new loop key. If a cluster header is caught, then its member nodes have to take part in a new cluster header’s election. At the same time, the probability of a cluster header being caught is determined by the result that cluster

Table 3. Cluster-based VS loop-based in node storage

| CBKMS | | LBKMS | |
|-----------------|---|---------------|--|
| Node function | Storage content | Node function | Storage content |
| Cluster header | Cluster ID Cluster key Cluster member IDs Neighbor clusters’ Ids A global key Node ID self | Loop creator | Loop key Link table(include loop sequence) A global key Node ID self A private key |
| Cluster members | Cluster ID Cluster key (some nodes) Neighbor clusters’ Ids A global key Node ID self | Loop members | Loop key Link table(include loop sequence) A global key Node ID self A private key |

Table 4. Node responsibility comparison between CBKMS and LBKMS

| CBKMS | | LBKMS | |
|-----------------|---|-----------------|---|
| Node identifier | responsibility | Node identifier | responsibility |
| Cluster header | 1.Generate Cluster ID and Cluster key; 2.key distribution; 3.Delete or add node; 4.Rekey without changing header | Loop creator | 1.Generate Loop key; 2.key distribution; 3.Broadcast loop sequence to neighbors; |
| Cluster members | 1.Aggregate sensor data with in-cluster neighbor; 2.Receive message from cluster header and reply; 3.Send data to header or neighbor nodes; 4.re-electing new cluster header | Loop members | 1.Aggregate sensor data with left and right neighbor; 2.Send data to left or right neighbor according to link table; |

Table 5. Comparison of probability of node being caught

| CBKMS | | LBKMS | | |
|-----------------|---|-----------------|--|----------------------|
| Node identifier | Probability being caught | Node identifier | Probability being caught | |
| Cluster header | $\frac{C_n}{T_n}$ | Loop creator | Before all loops being formed | same as loop members |
| | | | after all loops being formed | 0 |
| Cluster members | $\frac{(T_n - C_n)}{T_n}$ | Loop members | $\frac{1}{T_n}$ | |
| | Cn: Cluster numbers Tn: total node numbers | | Ln: loop numbers Tn: total node numbers | |

Table 6. Comparison of impact of node being caught

| CBKMS | | LBKMS | |
|---------------------------------|---|---------------------------------|---|
| identifier of Node being Caught | Impact to WSN | identifier of Node being Caught | Impact to WSN |
| Cluster header | Lost control to all the cluster members under the control of that cluster header; WSN have to start a new round cluster header election | Loop creator | same as loop members |
| Cluster members | The cluster header have to delete it from the member list and inform other members; The cluster header start a rekeying | Loop members | Neighbor nodes delete it from the link table and loop sequence; Neighbors nodes generate new loop key and spread it along the loop sequence |

numbers compare to the total node numbers. This probability is greater than that of a loop creator being caught. The probability comparison and impact comparison is listed in Table-5 and Table-6.

5 Conclusion

Key management is one of the most important technologies in the security mechanism of WSN. In this paper, we present a new key management scheme called LBKMS which integrates key pre-distribution mechanism in a loop-based infrastructure. LBKMS is also a dynamic scheme that can accommodate changing scenarios. The rekeying scheme based on loop topology and its security enhancement is also described in detail. Comparing with cluster-based key management schemes, LBKMS key management is proved to be more efficient, cost-saving and safe. Future research should focus on further reduction of communication cost in key establishment.

Acknowledgments

This work was supported by the National Research Foundation for the Doctoral Program of Higher Education of China under grant No. 20049998027, and the National Science Foundation of China under grant No. 90604006 and No. 90104001.

References

- [1] Carman, D.W., Kruus, P.S., Matt, B.J.: Constraints and approaches for distributed sensor network security. Technical Report #00-010, NAI Labs (2000)
- [2] Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: The 9th ACM conference on Computer and Communications, Washington, DC, USA, November 18-22, pp. 41–47 (2002)
- [3] Chan, H., Perrig, A., Song, D.: Random key pre-distribution schemes for sensor networks. In: Proc. 2003 IEEE Symposium on Security and Privacy, May 11-14, pp. 197–213 (2003)
- [4] Liu, D., Ning, P.: Establishing pairwise keys in distributed sensor networks. In: ACM Conference on Computer and Communications Security, pp. 52–61 (2003)
- [5] Du, W., Deng, J., Han, Y.S., Chen, S., Varshney, P.K.: A key management scheme for wireless sensor networks using deployment knowledge. In: INFOCOM 2004, vol. 1, pp. 586–597 (March 7-11, 2004)
- [6] Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J., Khalili, A.: A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. *ACM Transactions on Information and System Security* 8(2), 228–258 (2005)
- [7] Blom, R.: An optimal class of symmetric key generation systems. In: Beth, T., Cot, N., Ingemarsson, I. (eds.) EUROCRYPT 1984. LNCS, vol. 209, pp. 335–338. Springer, Heidelberg (1985)
- [8] Choi, S., Youn, H.: An Efficient Key Pre-distribution Scheme for Secure Distributed Sensor Networks. In: EUC 2005. LNCS, vol. 3823, pp. 1088–1097. Springer, Heidelberg (2005)
- [9] Li, Y., Wang, X., Baueregger, F., Xue, X., Toh, C.K.: Loop-Based Topology Maintenance in Wireless Sensor Networks. In: Lu, X., Zhao, W. (eds.) ICCNMC 2005. LNCS, vol. 3619, Springer, Heidelberg (2005)
- [10] Blundo, C., Santix, A D, Herzberg, A., Kuttan, S., Vaccaro, U., Yung, M.: Perfectly-secure key distribution for dynamic conferences. In: The 12th Annual International Cryptology Conference on Advances in Cryptology, pp. 471–486. Springer, Berlin (1992)
- [11] Vljajic, N., Xia, D.: Wireless Sensor Networks: To Cluster or Not To Cluster? In: IEEE International Symposium on WoWMoM 2006, Niagara-Falls, Buffalo-NY, USA (June 2006)
- [12] Chorzempa, M., Park, J.-M., Eltoweissy, M.: SECK: survivable and efficient clustered keying for wireless sensor networks. In: IPCCC 2005 (2005)
- [13] Younis, M.F., Ghumman, K., Eltoweissy, M.: Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks. *Parallel and Distributed Systems, IEEE Transactions* 17(8), 865–882 (2006)
- [14] Lin, L., Ru-chuan, W., Bo, J., Hai-ping, H.: Research of Layer-Cluster Key Management Scheme on Wireless Sensor Networks. *Journal of Electronics & Information Technology* 28(12) (December 2006)

A MAC Protocol with Little Idle Listening for Wireless Sensor Networks

Chaoguang Men^{1,2}, Yongqian Lu¹, and Dongsheng Wang^{1,2}

¹ Research and Development Center of High Dependability Computing Technology, Harbin Engineering University, Harbin, Heilongjiang, 150001, P.R. China

² National Laboratory for Information Science and Technology, Tsinghua University, Beijing, 100084, P.R. China
{menchaoguang, luyongqian}@hrbeu.edu.cn

Abstract. In wireless sensor networks, energy efficiency is crucial to achieving satisfactory network lifetime. To reduce the energy consumption significantly, a node should turn off its radio as long as possible. We propose a MAC protocol with little idle listening. The sensor node periodically turns on its radio in polling period and checks for a wake-up signal by sampling the energy on the channel. After polling period, the node enters the long sleep period. The data latency is reduced through reserving the channel in polling period. Analyses and simulations reveal that the proposed protocol outperforms S-MAC and LPL in energy conservation and latency.

Keywords: wireless sensor networks, protocol, media access control, energy efficient.

1 Introduction

Wireless sensor networks (WSN) consists of a large number of distributed nodes with sensing, data processing, and communication capabilities. These nodes are self-organized into a multi-hop wireless network and collaborate to accomplish a common task. As sensor nodes are usually battery-powered, and they are required to operate as long time as possible, so energy efficiency is critical in design of wireless sensor networks [1].

In this paper, we present a MAC protocol with little idle listening, named *L-MAC*, which not only out performs existing energy-efficient MAC protocols on energy conservation, it also mitigates the problem on hidden node interference through adopting a reasonable forwarding delay mechanism. Moreover, it has a better performance at the data latency.

The remainder of this paper is organized as follows: Section 2 discusses related work on energy-efficient of MAC layer in sensor networks. Section 3 describes the proposed protocol, and analyses the latency. Section 4 compares the performance of *L-MAC* with existing mechanisms via simulations. Section 5 concludes the paper.

2 Related Work

S-MAC is a protocol developed specifically to address energy issues in wireless sensor networks [2]. It uses a simple scheduling scheme to allow neighbors to sleep for long periods and synchronize wakeups. In *S-MAC*, nodes enter sleep mode when a neighbor is transmitting, and segment long packets to avoid costly retransmissions. While the periodic sleep may result in high latency, especially for multi-hop routing algorithms, since all intermediate nodes have their own sleep schedules. The control messages sent by the nodes, which are nearby the border of virtual cluster, are not very useful to hidden terminal problem, because the schedules are not synchronous. Furthermore, the nodes bordering two or more virtual clusters adopt different listen and sleep schedules, so they consume more power than the others and are apt to be disabled. *SUA* applies a schedule unifying algorithm to unify multiple schedules, which eliminates the influence of bordering nodes [3]. But the schedule unifying algorithm needs a lot of communications to realize it.

Low-power listening is presented in *B-MAC* [4]. The basic idea of low-power listening is to shift the cost from the receiver to the transmitter by increasing the length of a preamble. If a preamble is detected, the receiver will continue to listen until the start-symbol arriving and the message being properly received. If no preamble, the radio is turned-off again until the next sample.

TW-MAC proposes that energy can be conserved by amortizing the energy cost of communication over multiple packets [5]. In addition, the protocol allows sensors to control the amount of buffered packets since storage space is limited. The disadvantage of this protocol is that a busy tone must be transmitted before every data packet. This leads to energy waste and message latency. The double radios are too complicated for most sensor networks to implement.

LAS-MAC separates channel reservation process and data transmission process [6]. The nodes having data to forward are scheduled during reservation process. The other nodes with no schedule go to sleep to save energy. Only scheduled nodes are awake during scheduled time. The disadvantage of this protocol is that the nodes having data to forward must wait for next duty cycle when they overhear interference, but the channel may not always be busy in this duty cycle. The unnecessary waiting results in the decrease in throughput.

3 The MAC Protocol with Little Idle Listening (*L-MAC*)

In proposed protocol *L-MAC*, a duty cycle comprises of a polling period and a sleeping period, as shown in Fig.1.

In this MAC protocol, each node only periodically turns on its radio and checks for a wake-up signal by sampling the energy on the channel in polling period. Whether there is a wake-up signal can be determined within 50 μ s [7]. After this period, the node enters the long sleep period. A not precise synchronization mechanism is adopted, so that all nodes are able to synchronize in sleep period. The closer the distance between nodes is, the more precise the synchronization between them is. Based on these, *L-MAC* utilizes a spot of control messages for multi-hop channel reservations in polling period, and data messages are transmitted following the control

messages. The nodes having messages to forward adopt a reasonable forwarding delay mechanism to mitigate the problem on hidden node interference.

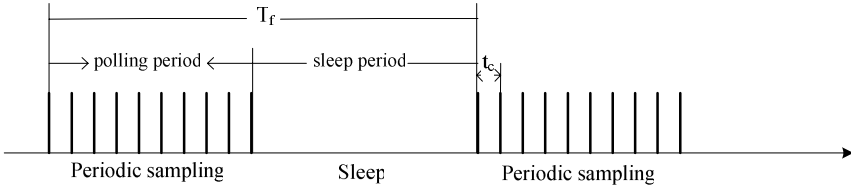


Fig. 1. The L-MAC duty circle

3.1 Description of L-MAC

We describe some terms as follow [8]:

- *Transmission range.* When a node is within transmission range of a sender node, it can receive and correctly decode the packets from the sender node.
- *Carrier sensing range.* Nodes in the carrier sensing range can sense the sender’s transmission. Carrier sensing range is typically much larger than the transmission range [9]. Note that the carrier sensing range and transmission range depend on the transmit power level.
- *Carrier sensing zone.* Carrier sensing zone is the range which excludes the transmission range from the carrier sensing range. When a node is within the carrier sensing zone, it can sense the signal but can not decode it correctly.

For brevity, we supposed that the carrier sensing range (radius) is one time larger than the transmission range [9].

Fig. 2 denotes the overview of L-MAC. As shown in Fig.2, when a source node (node-a) has data to be sent to the sink node (node-e), it has to wait till the polling period. In polling period, the sender continually sends control messages as preamble to wake up the receiver until the receiver is awoke and decodes the control message correctly. The interval between control messages is denoted by t_i .

$$t_i = nt_c + it_m. \tag{1}$$

In above formula, n is a random natural number, i is the times of retransmission, t_c is sampling cycle, t_m is the time of control message transmission. When node-a sends the control messages, its second hop neighbor (node-c) which is at the carrier sensing zone of node-a also has chance to sense the wakeup signal [8]. We can say that node-a is likely to help node-b to wake up node-c. This may reduce the control message of node-b. If receiver (node-b) received the control message successfully and it is not the sink node, it will forward the control message to the next hop neighbor (node-c). Node-a takes the control message sent by node-b as the virtual ACK which denotes that node-b has received the control message sent by node-a successfully. Then, if the control message needs to be forwarded further, the process is repeated until the sink node receives the control message successfully and returns an ACK packet. If retransmission times exceed the limit, the sender node will wait for the next polling

period to retransmit the control message. All the nodes received the control message will keep waking for a period to wait for the data packets. This is a channel reservation process.

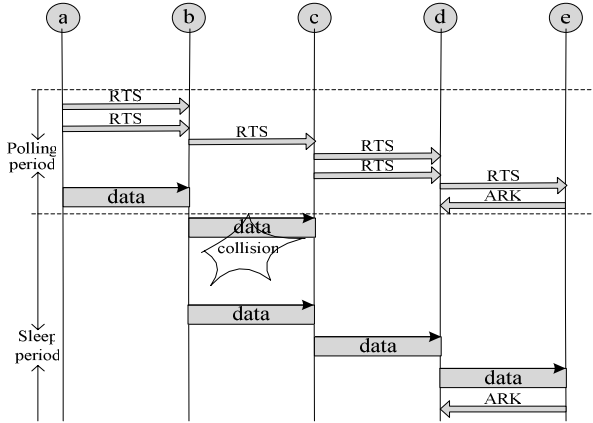


Fig. 2. Overview of L-MAC

The source node (node-a) prepares to send data packets after receiving the control message coming from node-b. The data packets forwarding mechanism can follow the control message forwarding mechanism during channel reservation process.

When a sender senses that the channel is busy, it needs to delay its transmission to mitigate the hidden node interference problem. Otherwise, overlapping transmissions caused by the transmitting node and the hidden node can lead to collision at the first hop node. For example, as shown in Fig.2, when node-a has a data packet to send, it doesn't transmit the packet immediately until node-d has completed the control message forward. Otherwise, overlapping transmissions caused by node-a and node-d can lead to collision at the node-b.

3.2 Latency Analysis

We also use the assumptions that adopted in [6]. There are N hops from the source to the sink. For hop n , we denote carrier sense delay by $t_{cs,n}$, transmission delay by t_{tx} , sleep delay by $t_{s,n}$ and a frame of main duty cycle by T_f .

According to reference [6], the overall delay of a packet over N hops in S -MAC is:

$$\begin{aligned}
 D(N) &= D_1 + \sum_{n=2}^N D_n \\
 &= t_{s,1} + t_{cs,1} + t_{tx} + \sum_{n=2}^N (T_f + t_{cs,n} - t_{cs,n-1}) \\
 &= t_{s,1} + (N-1)T_f + t_{cs,N} + t_{tx}.
 \end{aligned} \tag{2}$$

So the average latency of S-MAC without adaptive listen over N hops is:

$$\begin{aligned}
E[D(N)] &= E[t_{s,1} + (N-1)T_f + t_{cs,N} + t_{tx}] \\
&= T_f/2 + (N-1)T_f + t_{cs} + t_{tx} \\
&= NT_f - T_f/2 + t_{cs} + t_{tx}.
\end{aligned} \tag{3}$$

Equation (3) shows that the multi-hop latency also linearly increases with the number of hops in *S-MAC* when each node strictly follows its sleep schedules. The slope of the line is the frame length T_f .

In *L-MAC*, control packets are forwarded ahead to reserve channel. They are always much shorter than data packets. So the forwarding speed must be faster than the data packets. Considering that the polling period is long enough (i.e., 100ms), control message can be transmitted from source node to sink node within the polling period (we will discuss it in section 4). In addition, transmission rate control mechanism makes data packet lag control packet for four hops. In this case, the whole forwarding delay will comprise of three parts: sleep time t_s , four hops lag T_{lag} and data packet delay T_n .

Sleep time t_s is the same to *S-MAC*, the mean value is $T_f/2$.

Four hops lag is:

$$T_{lag} = 4(t_{cs} + t_{tx}). \tag{4}$$

In data packet delay period, all the nodes in the link are awake. When a node receives a packet, it immediately starts carrier sense and tries to forward it to the next hop. The average delay at hop n is $t_{cs,n} + t_{tx}$. The entire data packet delay over N hops is:

$$D(N) = \sum_{n=1}^N (t_{cs,n} + t_{tx}). \tag{5}$$

So the average data packet delay over N hops is:

$$E[D(N)] = N(t_{cs} + t_{tx}). \tag{6}$$

The total latency of *L-MAC* is:

$$\begin{aligned}
E[t_s + T_{lag} + D(N)] &= E[t_s] + E[T_{lag}] + E[D(N)] \\
&= T_f/2 + 4(t_{cs} + t_{tx}) + N(t_{cs} + t_{tx}) \\
&= T_f/2 + (N+4)(t_{cs} + t_{tx}).
\end{aligned} \tag{7}$$

We can see that the average latency in *L-MAC* still linearly increases with the number of hops. Now the slope of the line is $t_{cs} + t_{tx}$. It is much smaller than the slope of *S-MAC*.

4 Simulations and Performance Evaluation

We run simulations using *OPNET*. Except for *L-MAC*, we also implement three MACs for comparison, i.e., a simple version of *S-MAC* without its synchronization and message passing scheme, *LPL* and full active *802.11 MAC*. The last one will serve as the baselines of latency, energy and delivery ratio. All the sleep scheduled

protocols have the basic duty cycle of 10%. In *L-MAC*, the polling period is subdivided into 50 sampling periods, and the sampling time is the same as *LPL* ($50\mu s$). The polling period of *L-MAC* is $100ms$, it is the same long as the listen period of *S-MAC*. We set the bandwidth to $115kbps$. Each data packet size is 150 bytes, and control packet size is 15 bytes. 100 nodes are deployed randomly in an area of $300 \times 300m^2$. The radio range (radius) is 30m. The carrier sensing range (radius) is 65m. We choose three source nodes and one sink node from different corners. We use the same energy consumption model as in [10] for the radio hardware.

We choose 3 metrics to evaluate the performance of *L-MAC*. Energy cost is the total energy cost to deliver a certain number of packets from sources to sink. This metric shows the energy efficiency of the *MAC* protocols. Latency is the end to end delay of a packet. Delivery ratio is the ratio of the number of packets arrived at the sink to the number of packets sent by sources.

Fig. 3 shows the averaged packet latency with different hop length. In *L-MAC*, *LPL* and full active *802.11 MAC*, the latency of them increases with the number of hops. Their increasing exponentials are almost the same. Compared with *LPL* and *8.2.11 MAC*, the additional latency of *L-MAC* comes from the sleep delay at the first hop. *LPL* only has a short additional preamble at each hop, so its latency gap compared with *802.11 MAC* is not obvious. As the *S-MAC* protocol has sleep delay at every hop, it has a higher latency.

Fig. 4 shows the energy cost with different hop length in one data stream. In all *MAC* protocols, the energy cost increases linearly with the number of hops. However, the energy cost of the full active *802.11 MAC* increases much faster than other three *MAC* protocols, because *S-MAC* has some additional active periods. The additional active periods come from the nodes which are not the receiver but within the overhearing range. *L-MAC* consumes less energy than *S-MAC* and *LPL*. The reason is that it has a longer sleep time.

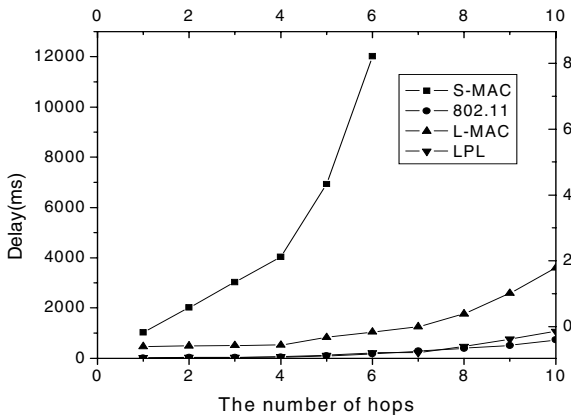


Fig. 3. Mean packet latency on each hop under low traffic load

We then test the traffic adaptation of these *MAC* protocols, by varying the sensor report interval on the source node from 0.2s to 6s. In all, thirty packets are sent at the source nodes. The simulation time is 1000s.

Fig. 5 shows the averaged packet latency for different source report intervals. Clearly, full active 802.11 MAC has the lowest latency. Due to the preamble and the initial sleep delay at the source nodes, LPL and L-MAC have a slightly higher latency. S-MAC, however, has much higher latency, especially when traffic load is heavy. The reason is that the packets in S-MAC can be forwarded only one hop during each duty cycle, and packets suffer from both sleep delay and queuing delay. When traffic load is very high, collisions would significantly increase packet latency, because retransmission can only be done after one total duty cycle.

Fig. 6 shows the total energy cost for different source report intervals. On the condition that the total numbers of packets are the same, the energy consumption is almost invariableness. However, the energy cost may slightly increase when the traffic load becoming heavier, it is due to that the retransmission wastes some energy.

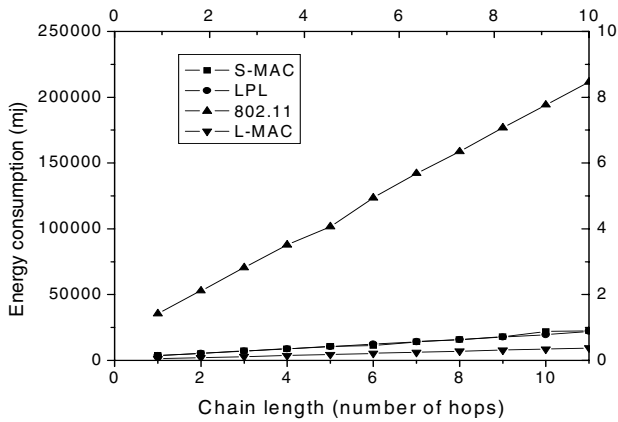


Fig. 4. Total energy consumption on each hop under low traffic load

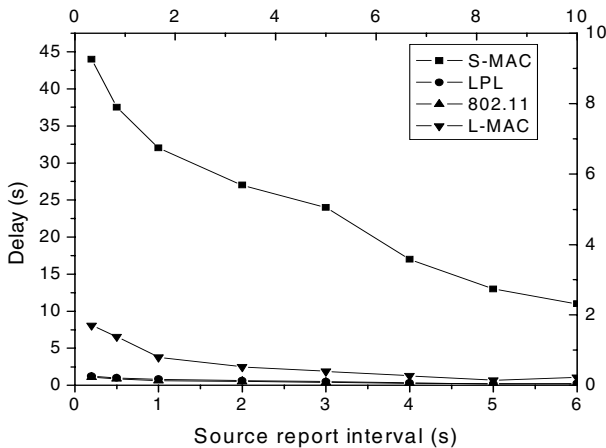


Fig. 5. Mean packet latency under different source report interval

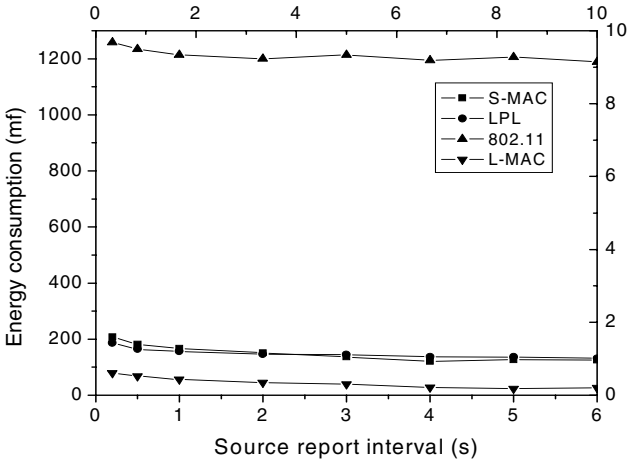


Fig. 6. Energy consumption under different source report interval

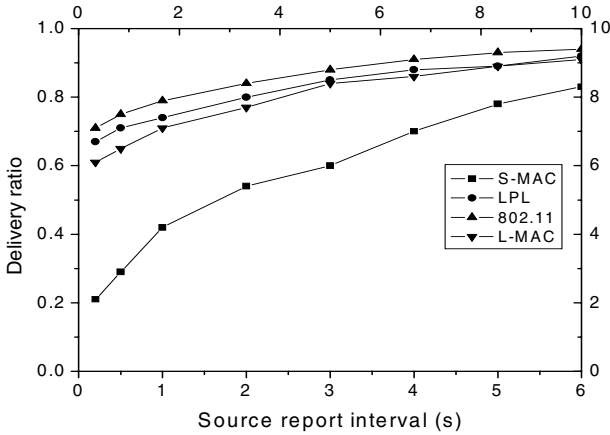


Fig. 7. Throughput under different source report interval

Fig. 7 shows the throughput for different MAC protocols. *802.11* MAC and *LPL* have the best data throughput. *L-MAC* also has a better performance. Compared with full active *802.11* MAC, it is good enough for wireless sensor networks.

5 Conclusions

This paper presents a novel MAC protocol for wireless sensor networks. Compared to *S-MAC* and *LPL*, it makes following improvements: minimizing the idle listening, accelerating the data passing, adopting a powerful forwarding delay mechanism to

mitigate the hidden node interference problem. The simulation results reveal that our protocol has better performance in packet delivery ratio, latency and energy efficiency.

References

1. Demirkol, I., Ersoy, C., Alagoz, F.: MAC Protocols for Wireless Sensor Networks: A Survey. *IEEE Communications* 44(4), 115–121 (2006)
2. Ye, W., Heidemann, J., Estrin, D.: Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks. *IEEE/ACM Transactions on Networking* 12(3), 493–506 (2004)
3. Lee, W., Lee, D., Lee, H.S.: Life Extension of Border Nodes in SMAC-based Wireless Sensor Networks by Unifying Multiple Sleep Schedules among Adjacent Virtual Clusters. *PE-WASUN, Canada*. vol. 10, pp. 267–268 (2005)
4. Polastre, J., Hill, J., Culler, D.: Versatile Low Power Media Access for Wireless Sensor Networks. In: *SenSys 2004, Maryland, USA*, vol. 11, pp. 95–107 (2004)
5. Miller, M.J., Vaidya, N.H.: A MAC Protocol to Reduce Sensor Network Energy Consumption Using a Wakeup Radio. *IEEE Transactions on Mobile Computing* 4(3), 228–241 (2005)
6. Kim, J., Park, K., Shin, J.-H., Park, D.: Look-Ahead Scheduling For Energy-Efficiency and Low-Latency in Wireless Sensor Networks. In: *PE-WASUN 2006, Spain*, vol. 10, pp. 141–144 (2006)
7. Hill, J.L., Culler, D.E.: Mica: A Wireless Platform for Deeply Embedded Networks. *IEEE Micro* 22(6), 12–24 (2002)
8. Jung, E.-S., Vaidya, N.H.: A Power Control MAC Protocol for Ad Hoc Networks. In: *Proceedings of the IEEE/ACM MobiCom Conference*, vol. 9, pp. 36–47 (2002)
9. Kamerman, A., Monteban, L.: WaveLAN-II: A High-Performance Wireless LAN for The Unlicensed Band. *Bell Labs Technical Journal* 2(3), 118–133 (1997)
10. Lin, P., Qiao, C., Wang, X.: Medium Access Control with a Dynamic Duty Cycle for Sensor Networks. In: *WCNC 2004/IEEE Wireless Communications and Networking Conference*, vol. 3, pp. 1534–1539 (2004)

Security Technologies Based on Home Gateway for Making Smart Home Secure

Geon Woo Kim¹, Deok Gyu Lee¹, Jong Wook Han¹, and Sang Wook Kim²

¹ Electronics and Telecommunications Research Institute
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{kingw, deokgyulee, hanjw}@etri.re.kr

² Kyungpook National University
1370, Sankyuk-dong, Buk-gu, Daegu, 702-701, Korea
swkim@cs.knu.ac.kr

Abstract. As home network is expanding into ubiquitous computing environment and lots of private information is accessible, it is required to protect home network system from illegal accesses and security threats in open network. In general deployment of home network, a secure home gateway is located at the boarder of each home and regarded to be a core entity providing services and controlling traffic. So in this paper, we propose a security system guaranteeing security, availability, and reliability based on the secure home gateway and describe our implementation on home network including authentication, authorization, and security policy.

Keywords: Home Network, Smart Home, Security, Authentication, Authorization, Access Control, Security Policy.

1 Introduction

Home network is a new IT technology environment for making an offer of convenient, safe, pleasant, and blessed lives to people, making it possible to be provided with a variety of home network services by constructing home network infrastructure regardless of deices, time, and places. This can be done by connecting home devices based on a variety of communicating network protocols, such as mobile communication, Internet, and sensor network [1]. With the home network, we can easily control home devices, make use of a number of services such as a VOD service, a remote health care service, a T-commerce service and etc.. Namely, home network can be defined to be a total home information system providing a number of services and solutions, not just simple networking within single home.

Unfortunately, home network is subject to be infected by all legacy security threats existing in open network since it is accessible from open network and a variety of network protocols coexist, where each network contains its own security threats.

Especially, as home network consists of heterogeneous network protocols and a variety of service models, it is likely to be exposed to various cyber attacks of Internet, involves hacking, malicious codes, worms, viruses, DoS attacks, and eavesdropping since it is connected to Internet [2].

So in this paper, we propose an integrated security system to guarantee reliability, availability, and security based on secure home gateway and describe our implementation including authentication, authorization, and security policy.

2 General Model for Home Network

Home network comprises a number of factors of legacy networks and systems.

The categorization of above entities consisting home network is from ITU-T Recommendation X.1111 regarding “Framework of Security Technologies for Home Network”.

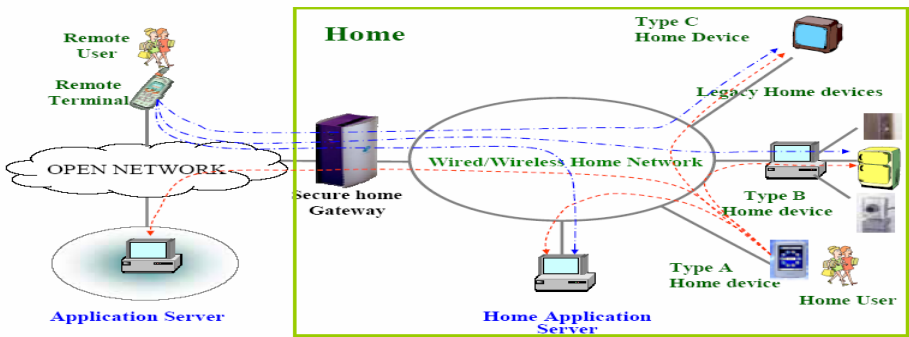


Fig. 1. General model for home network

Figure 1 describes general model for home network from X.1111 [3].

All security requirements and technologies must conform to the above model.

3 Necessities of Security for Home Network

As we mentioned in the previous section, home network is likely to contain a number of security threats that are possible in legacy applications.

3.1 Target of Existing Attacks Due to Connection to Internet

Because home network is composed of heterogeneous network protocols, it is subject to be a target of existing attacks, where every process working in the Internet can access the home network. Each network protocol has its own features and security threats as shown in Figure 2.

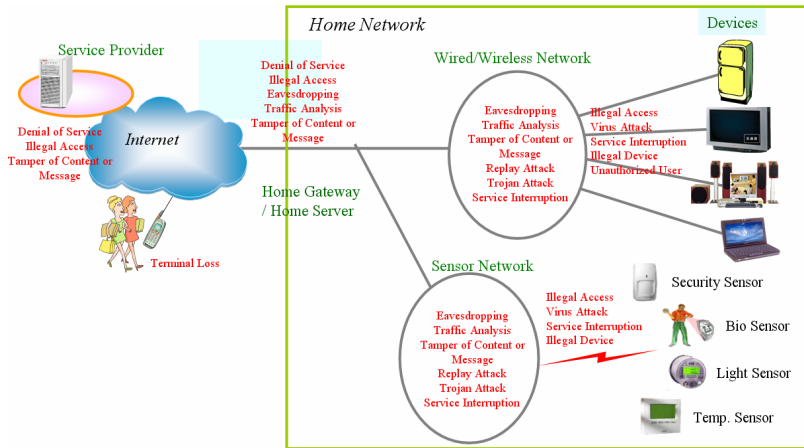


Fig. 2. Security threats in home network

3.2 Trusted Relationships Among Entities

In order to make home network reliable, safe, and available, how to establish trusted relationships among entities that are deployed in home network is most important from security point of view. Especially, in ubiquitous home network environment, majority of services are based on communications among home devices.

During communications among home devices, some exchanged information is supposed to be critical when revealed to others. For example, in remote health-care service, tamper or modification to vital information is closely related to the breath of life and personal medical information known to other untrusted entities may result in serious privacy violation.

Furthermore, it is possible to make a new attack by collecting and reasoning the behavior patterns or habits.

3.3 Others

There is an evolution to be ubiquitous environment of home network, and each device tends to be light-weight following the movement. In ubiquitous environment, it seems to be infrastructureless, where security is getting a more important requirement.

And there is an increment of requirement for security. For example, the Intel and the Verisign are establishing strong security infrastructure by enforcing device authentication.

Also, security for home network is required to be convenient and needs minimum interventions by home users.

4 Security Technologies for Home Network

There are some security technologies for making home network secure. Among them, authentication and authorization are expected to be essential.

In ubiquitous home network environment, each entity, which is an object of authentication including a user or a device involved in home, is subject to move into other domains such as other home network domains, telematics service domain, and ubiquitous sensor domain. The authentication module must support above circumstance and relative requirements.

There are a few authentication mechanisms used for home network. They can be categorized into two layers: authentication mechanisms for intra-domain, and authentication mechanisms for inter-domain.

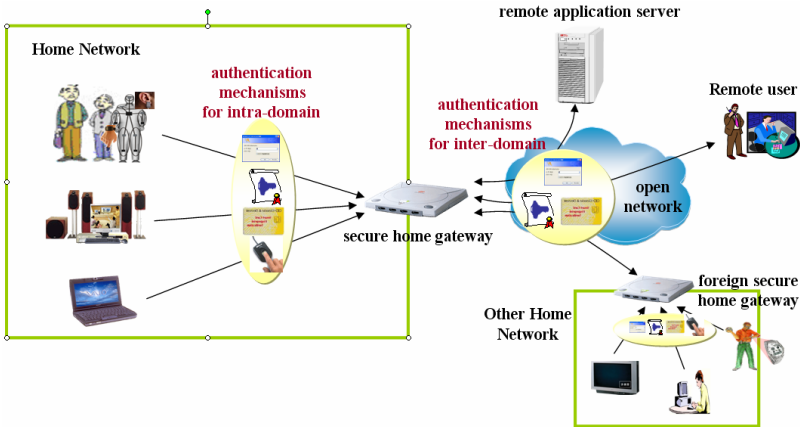


Fig. 4. Authentication mechanisms for ubiquitous home network

For authentication within single home domain, most of the existing authentication mechanisms such as ID-password-based authentication mechanism, certificate-based authentication mechanism, smart card-based authentication mechanism, and biometric-based authentication mechanism, can be used. The decision to adopt which authentication mechanism is depending on application.

On the other hand, it is desirable to exclude the biometric-based authentication from inter-domain security. In case of using other types of authentication mechanisms, even though secret information is revealed to others, we may just change it. But biometric information is not changeable. Therefore, it results in serious privacy violation when disclosed.

Each user is required to be authenticated just one time to access every home network service. Namely, each user is authenticated by a secure home gateway and doesn't consider the following authentication process. For example, when a user is to access a remote application server and the remote application server performs its own authentication, the user is identified by the secure home gateway and the secure home gateway does authentication with the remote application server instead of the user.

For making it possible, the secure home gateway contains an authentication mapping function, which enables mapping between authentication mechanisms for intra-domain and authentication mechanisms for inter-domain.

4.2 Authorization

The purpose of authorization is controlling access of entity even though it has been successfully authenticated and restricting a privilege and access right. Also, it can minimize the loss when home network system is penetrated and attacked by malicious accesses or unauthorized uses.

We can use an ACL (Access Control List) or a RBAC (Role-based Access Control). The ACL directly established relationships between subjects and resources, where a subject means an entity that is accessing, and a resource an entity that the subject is accessing. The ACL is simple so useful for relatively small-scale network. On the other hand, The RBAC adapts an intermediate component called a role between a subject and a resource, so indirectly sets up relationships between them. The RBAC seems to be adequate for relatively large-scale network.

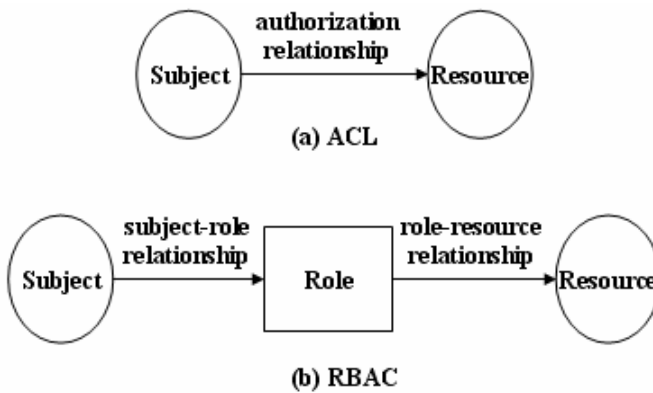


Fig. 5. ACL vs. RBAC

Figure 5 simply illustrates ACL and RBAC.

As home network includes a variety of network protocols and is expected to support many service models such as a client-server model, a peer-to-peer communication model, and hybrid model, it is difficult to definitely decide which mechanism is suitable for home network. Actually we had better use a different authorization model according to the specific home network service. As a result, we need an integrated authorization framework for home network.

Figure 6 shows an integrated authorization framework for home network.

Existing authorization mechanisms can be categorized into three fields: server-based authorization mechanism, peer-to-peer authorization mechanism and certificate-based authorization mechanism. A server based authorization mechanism works on client-server model and the server generates and maintains authorization rules, enforces it. This method is relatively simple and easy to apply. A peer-to-peer authorization mechanism is for p2p communication service model. A peer can manage authorization rules by itself or require help of designated authorization server. This model is relatively complicated to implement and there are a few constraints considering database maintenance and H/W specifications of peer device and etc., A certificate-based authorization mechanism is generally used in open network and conforms to the PKI.

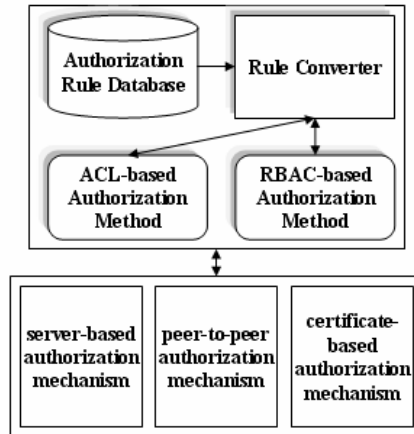


Fig. 6. Integrated authorization model for home network

These mechanisms define their own schema to specify the authorization rules, which may be of either an ACL or a RBAC.

Authorization Rule Database contains raw authorization rules and the details are not described in this paper. Rule Converter translates the raw authorization rules into ACL-based authorization rules or RBAC-based authorization rules and the reverse. Also, it can maintain consistent authorization rules between ACL-based authorization method and RBAC-based authorization method by reflecting the changes of one type of authorization rules to the other type of authorization rules immediately.

Authorization model for home network comprises an access control definition module, an access control enforcement module, an information collection module, an access control database, and a log database.

Figure 7 shows the functional components for authorization.

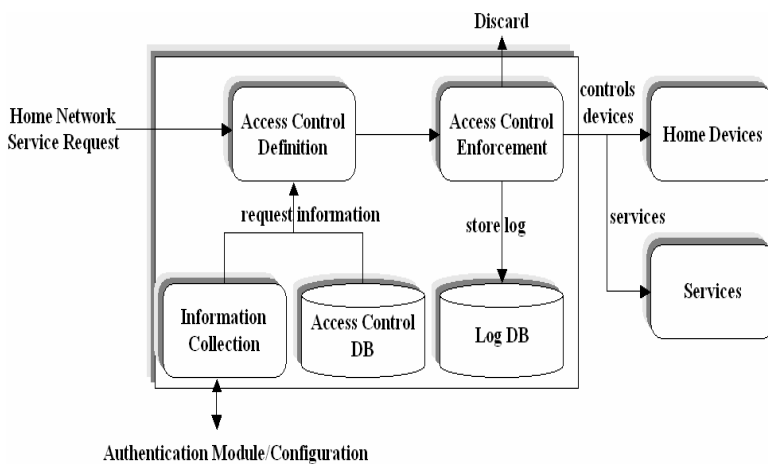


Fig. 7. Functional components for authorization

4.3 Security Policy

Security policy is a set of single rule consisting of *condition* and *action*. Whenever a condition is satisfied, action is performed, where the key issue is how to construct condition. Elements to be contained in condition are as follows

- Time(date, day, duration)
- Event(sensor, user-triggering, state)
- Log(statistics)

Also, we define relationships (interaction, union) among above elements and support recursive structure, which makes it possible to build complex conditions.

Time and event are the basic elements of condition and can be generally used. On the other hand, log-based condition controls access by statistics information. For example, there is a pre-condition that the security policy manager set the policy that children could not use the game service more than 30-hour in a month. Whenever the children access the game service, their usage information may be store at log database. If the above condition is satisfied, connection would be rejected and they can't access it during the month.

Action contains controlling device and providing home services and etc. In order to control device, it should cooperate with corresponding middleware used by controlled device such as UPnP, LnCP, zigbee, UWB, etc.

Figure 8 shows the conceptual architecture and operations on security policy enforcement for home network.

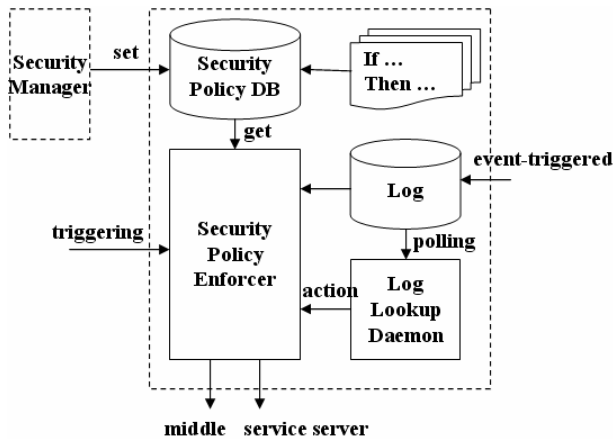


Fig. 8. Security policy system for home network

Security policy manager generates and manages the security policy specialized for home network which includes authentication policy, authorization policy and other types of security policy.

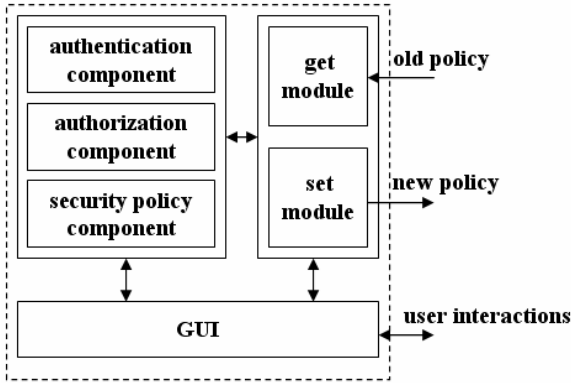


Fig. 9. Security Policy Manager for home network

Considering the features of home network, it must be enough easy for non IT-familiar user to use. In our system, we use a Drag-and-Drop mechanism to establish the security policy, so anyone can handle it if he has been authenticated successfully.

Figure 9 illustrates the functions that the security policy manager provides.

In our system, we use a new defined language called an xHDL (extensible Home security Description Language) based on XML [9].

5 Implementation

This section describes the implementation of security for home network.

Figure 10 shows entities the their relationships in our implementation.

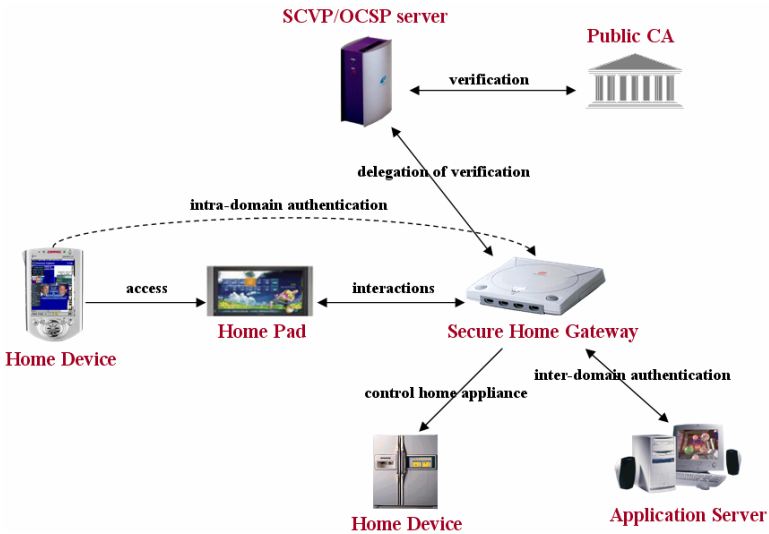


Fig. 10. Structure of our implementation

With the above structure of implementation, authentication flow when using device certificate is shown in Figure 11.

For using certificate, the home device must be issued it by the public CA with the helps of the Home Pad and the Secure Home Gateway. When verifying the certificate, our system uses the delegated server involving SCVP and OCSP, which is regarded to

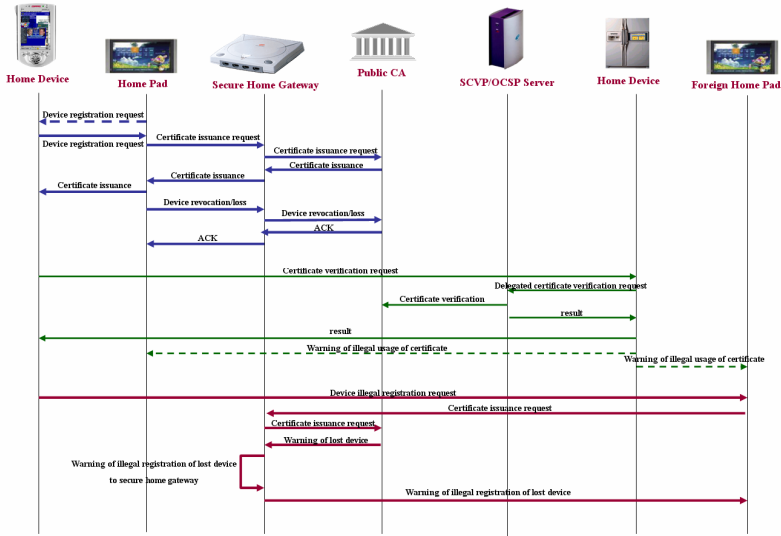


Fig. 11. Authentication flow when using device certificate

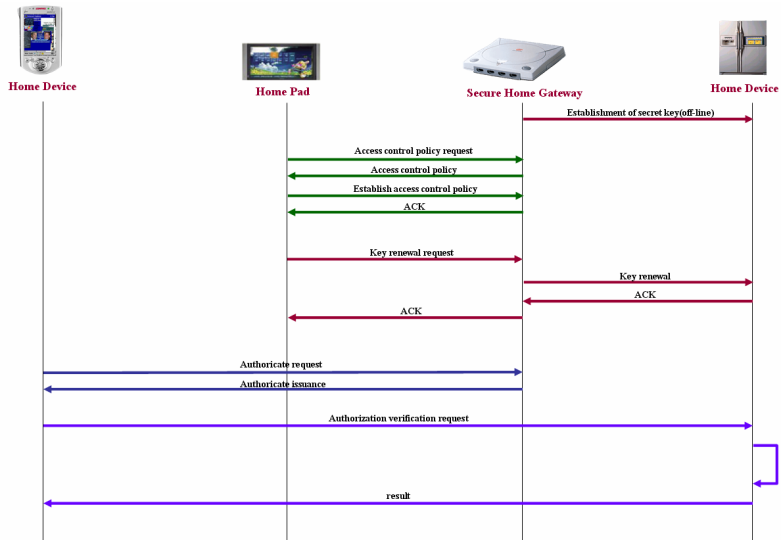


Fig. 12. Authorization flow when using authenticare

reduce the computation overhead by home devices with relative low capacities. Also, our system provides a mechanism preventing illegal usage/registration when lost.

Figure 12 shows authorization flow when using an authoricate, which is another type of certificate for authorization.

Once the home device is successfully authenticated, an authoricate is issued to it for access control. With it, the home device can control other home device without additional authentication. Also, each home device is expected to perform the authorization process since it needs to execute just symmetric key-based encryption algorithms.

6 Conclusion

Since home network consists of heterogeneous network protocols and contains existing security threats and holes of Internet such as hacking, malicious codes, worms, viruses, DoS attacks and eavesdropping, due to connections to the open network, we need a security framework to safeguard against them, efficiently guarantee reliability and availability.

So in this paper, we propose home network security technologies including authentication, authorization, and security policy and describe our implementation.

An authentication mechanism authenticates entity that is access home network. Also we can select our favorite authentication method such as ID-password-based authentication method, certificate-based authentication method, and biometric-information-based authentication method.

An authorization mechanism controls access by an entity even though it has been successfully authenticated already and restricts a privilege and access right. When some authenticated user wants to use home network service, the authorization mechanism receives identity-related information from corresponding authentication mechanism and looks for an adequate authorization rule in security policy database of security policy mechanism. Based on the found rule, the access control enforcer does authorization and informs the result to the entity. It may use both ACL and RBAC simultaneously. We propose an integrated authorization framework, where a variety of authorization methods can work collaboratively, and we do not have to care about the specific authorization method.

Security policy specifies the strategy for home network and provides basic rules for other security mechanisms such as authentication mechanism, authorization mechanism, and enforces security policy. In order to efficiently describe the security policy for home network, we define a new language called an xHDL (eXensible Home security Description Language).

References

1. Han, J.-W.: Revitalization Policy of Home Network Industry, 22nd edn., vol. 9, Korea Information Science Society (2009)
2. Han, J.-W., Kim, D.-W., Joo, H.-II.: Considerations for Home Network Security Framework. In: Korea Information Science Security, 22th edn., vol. 9 (September 2004)

3. Framework of security technologies for home network, ITU-T Recommendation X.1111 (2007)
4. Lee, Y.-k., Ju, H.-i., Park, J.-h., Han, j.-w.: User Authentication Mechanism Using Authentication Server in Home Network. In: Proceedings of the 8th International Conference on Advanced Communication and Technology
5. Lee, H.-k., Lee, Y.-k., Ju, H.-i., Han, J.-w.: User Authentication Mechanisms for Home Network using Home Server, TTAS.KO-12.0030
6. Abobo, B., et al.: Extensible Authentication Protocol (EAP)., IETF RFC3748 (June 2004)
7. Fund, P.: EAP Tunneled TLS Authentication Protocol, IETF draft-funk-eap-ttls-v1-00 (February 2005)
8. Palekar, A.S., Salowey, D., Zhou, J., Zorn, H.: Protected EAP Protocol (PEAP) version 2, IETF draft-josefsson-pppext-eap-tls-eap-10 (2004)
9. Kim, G.-W.: eXtensible Home Security Description Language. Telecommunications and Technologies Association (2006)

Layered Peer to Peer Streaming Using Hidden Markov Models

Sheng-De Wang and Zheng-Yi Huang

National Taiwan University, Taipei, Taiwan
{sdwang, d95921017}@ntu.edu.tw
<http://www.ee.ntu.edu.tw/>

Abstract. A fundamental problem in peer-to-peer streaming is how to select peers from a large network to request their media data. Due to the heterogeneity and the time-varying features of shared resources between peers, an adaptive method is required to select suitable peers. In this paper, we use Hidden Markov Models (HMMs) to model each peer to reflect the variation of resources. Among peers with different HMMs, the one which produces the maximum observation probability is selected as the serving peer. Through simulation results, we show that the proposed algorithm can achieve a good streaming quality and low communication overhead. In addition to these characteristics, the proposed model also comes with the fairness property.

Keywords: Peer to Peer, Streaming, HMM.

1 Introduction

Ubiquitous computing is a trend of current technology and the emergence of peer to peer networking makes it possible to achieve it, since P2P renders each peer as a server which can offer service to others. Besides that, the peer-to-peer paradigm offers an alternative possibility for streaming media over the network due to an important inherent characteristic: resources are shared among peers. Peers that simultaneously function as both clients and servers share their resources, such as computing power, bandwidth, storages and contents with others. This important characteristic avoids dedicated replication servers altogether and hence it does not have the bottleneck of client/server streaming architecture. A peer-to-peer media streaming system is operated in a kind of play-while-downloading mode [2]. An element of diversity is that the local storage of each peer is leveraged as a cache-and-relay mechanism in which requesting peers request media data and cache the most recently played media data during streaming [5]. The cached content can then be relayed to later peers that request the same content. But the most distinct feature of all is that from peer-to-peer streaming systems, users not only enjoy the availability of media contents but also the high quality of media streaming. The media streaming quality depends on many factors, ranging from the characteristics of the streaming sources, such as link capacity, availability, accessible bandwidth and overlapping of paths from multiple sources to receivers [8]. It is obvious that the peer selection policy plays an important role in peer-to-peer streaming.

In peer-to-peer multimedia streaming, the peer selection problem is how a peer selects a subset of peers from the network and request data from those selected peers, such that the desired media content could be received before their scheduled playback time in order to obtain a better streaming quality. The importance of the peer selection problem comes from that different outcome of selection would cause the different received time of data since peers have different capability to deliver data. Moreover, the different received time of data would result in a different streaming quality since the data received time is an important factor that affects the availability of data when they are needed. The difficulty of the selection problem follows from the heterogeneity and uncertainty of peers. Peers have varying bandwidths, diverse computation power and different buffered media contents. In addition, peers might come and leave in an unpredictable fashion and their resources vary with time. Therefore, a static and unadaptable approach to the peer selection problem will not work in the peer-to-peer streaming environment.

In this paper, we use a hidden Markov model (HMM, [1]) to model the bandwidth usage in the peer selection problem. That is, Peers are modeled as HMMs in which states represent status of bandwidth usage. A hidden Markov model is defined by a five-tuple, $\lambda = (N, A, B, K, \pi)$. N is the number of states in the model. A is state-transition probability distribution which is related to the distribution of offered bandwidth of neighbors. B denotes the observation symbol probability which depends on the state of a peer. The observation probability would be higher in a rich-bandwidth state than in a deficit-bandwidth state. K defines observation symbol, $\{0, 1\}$. The observation symbol 1 denotes that a peer is able to satisfy a request, 0 otherwise. π is the initial probability for each state. Before selecting a serving peer, a requesting peer would establish HMMs for some peers from its neighbors. With having a good streaming quality, the requesting peer initially set the observation $O = \{1\}$ with $|O|$ is arbitrarily in length and select a peer with maximum $P(O|\lambda)$, the highest observation probability, as the serving peer. Based on a layered streaming model, peers use the HMM streaming algorithm would obtain a high streaming quality and the fairness of the network. Moreover, the communication overhead incurred from the HMM streaming model is smaller as compared with other selection strategies.

The rest of this paper is organized as follows. Section 2 presents the assumed streaming model and our previous layered streaming model which the HMM streaming algorithm based on. Section 3 describes our solution to peers selection using hidden Markov model. Parameters of a HMM is also defined in detail in this section. Section 4 presents the simulation results. Related works are described at Section 5. Finally, Section 6 is the conclusion and our future work.

2 Layered Streaming

In our streaming model, we use layered coding to generate the media content. Briefly, layered coding mechanisms generate a base layer and n enhancement layers. The base layer is necessary for the media stream to be decoded, enhancement layers are applied to improve stream quality. The base layer can be decoded independently; however enhancement layers must be decoded based on subordinate layers. That is, the first

enhancement layer depends on the base layer and each enhancement layer $j + 1$ depends on its subordinate layer j , $1 \leq j \leq n - 1$. To simplify the notation, we call the base layer as layer 1. When we mention an n layer media streaming architecture, it is known that 1 to n layers are all taken into account. And we use R_n to denote the playback rate of an n layer media content. A media content is partitioned into sequential segments which are coded with layered coding. A segment is the unit for requesting, sending and playback.

In addition to layered coding, peers are structured into layers according to the bandwidth they offer to the network. We use $L(P_i)$ to denote the layer of peer i , and is defined by

$$L(P_i) = j \text{ if } (R_j) \leq \text{Bandwidth}_o < (R_{j+1})$$

For peer P_i of layer j , the offered bandwidth (or called up-streaming bandwidth) of P_i must at least be larger than R_j . For peer P_i of layer j , the largest layer of media it can request is restricted to j . Each peer is assigned a priority based on layer number. The larger the layer number, the higher the priority it has. When two or more peers contend with the bandwidth of a sending peer, the higher priority peer would have the right to use the resource first.

3 Peer Selection Using HMM

In this section, we describe how to use hidden Markov model to solve the peer selection problem. First, we define a set of peers for each requesting peer P_r that can serve as serving peers. This set is related to layers of neighbors of P_r and its own layer number.

Definition 1. *Let $S(P_r)$ be the set of selectable peers of P_r such that P_r could request data from those peers and we have the following definition*

$$S(P_r) = \{P_s : L(P_r) \leq L(P_s)\} \text{ for all } P_s \in P_r\text{'s neighbors}$$

When P_r performs the peer selection, P_r could only select peers from $S(P_r)$ as serving nodes.

Since each peer P_s is of limited bandwidth, and bandwidth of P_s varies with time. Each requester, moreover, selects its senders in a distributed fashion. Therefore, it is possible that actual bandwidth of a selectable peer might not coincide on the local information known by a requesting peer. When such situation happens, the requester might not obtain its desired media content if the requested target can't afford enough bandwidth to satisfy requests and the streaming quality of requester, therefore, would decline. To solve this mismatch problem, variation of bandwidth should be taken into account. In this paper, we use HMM to solve this problem. Based on layered streaming model, HMM is used as a statistical model and use the result of HMM as a reference to select the most suitable sending peer. In the following content, P_r is known as a requesting peer who will request data from some other peers; P_s is known as some peer from the selectable set of P_r that P_r might select it as its serving node.

In our layered HMM streaming model, each P_s was modeled as a hidden Markov model which is defined by a five-tuple, $\lambda = (N, A, B, K, \pi)$. N is the number of states in the model. In our current work, two states are defined for each P_s that are named as *GOOD* state and *BAD* state, they will be abbreviated to *G* and *B* respectively. From

the perspective of P_r , P_s might be in either *GOOD* state or *BAD* state. If P_r assumes that P_s is in *GOOD* state, then P_r thinks P_s might have enough bandwidth to satisfy its request. Otherwise, P_r thinks P_s might be short of bandwidth. Since bandwidth of P_r varies with time, the state of P_r would also change with time and such variations can be defined by state-transition probability distribution, $A = \{a_{ij}\}$ where

$$a_{ij} = P(\text{State}_{t+1} = j | \text{State}_t = i), i, j \in \{\text{GOOD}, \text{BAD}\}$$

is the probability that state i at time t would transit to state j at time $(t + 1)$. For example, a_{GB} represents the transition-probability from *GOOD* state to *BAD* state. Since in the our layered model, peers could only be requested by peers from lower layer and a priority mechanism is applied, the state-transition probability distribution A is, therefore, related to layer distribution of neighbors of P_s and the layer of P_r . Then A for P_s from the perspective of P_s is defined as

$$a_{BB} = a_{GB} = \frac{|C_{P_j}|}{|\text{Neighbors}_{P_s}|}, C_{P_j} = \{P_j : L(P_r) < L(P_j) < L(P_s)\}$$

Once a_{BB} and a_{GB} are defined, a_{GG} and a_{BG} could be defined as

$$a_{GG} = a_{BG} = 1 - a_{BB}$$

Neighbors_{P_s} denotes neighbors of P_s , C_{P_j} is a set that counts potential peers that might compete P_s with P_r . Hence, a_{BB} is the relative frequency that represents ratio of peers that might cause P_s to fail in receiving data. The more peers that might compete P_s with P_r , the more likely that P_s would stay in *BAD* state. Otherwise, fewer peer would compete with P_r and thus *GOOD* state would more precisely describe the actual bandwidth of P_s .

The observation symbols K , is defined as $K = \{0, 1\}$. The symbol 1 denotes that a request could be satisfied and 0 denotes otherwise. Hence, in order to get a best streaming quality, each requesting peer is expected to obtains an observation $O = \{1\}$ such that $|O|$ is as maximum as possible.

Since P_s might send data to P_r based on whether it can afford P_r 's desired bandwidth or not, the observation probabilities are, therefore, dependent on states. The observation probability distribution $B = \{b_j(k)\}$ denotes the probability of each state to deliver data. $b_G(1)$ is the probability to satisfy a request when P_s staying at *GOOD* state. Similarly, $b_B(1)$ is the probability to deliver data when P_s staying at *BAD* state. Since *GOOD* state denotes that P_r would have higher probability to get desired data, therefore, the initial value of $b_G(1)$ would be between the range as

$$0.5 \leq b_G(1) \leq 1$$

Similarly, for *BAD* state of P_s , the initial value of $b_B(1)$ would be defined as

$$0 \leq b_B(1) \leq 0.5$$

Once $b_G(1)$ and $b_B(1)$ are defined, $b_G(0)$ and $b_B(0)$ could be defined as

$$b_G(0) = 1 - b_G(1), b_B(0) = 1 - b_B(1)$$

When P_r establishes HMM for P_s for the first time, P_r random choose a value between $[0.5, 1]$ for $b_G(1)$ and a random value from the range $[0, 0.5]$ for $b_B(1)$. The initial probability of each state is set to equal, namely $\pi_G = \pi_B = 0.5$. However, when P_r re-establishes HMM for P_s later, P_r would set $b_G(1)$, $b_B(1)$ and initial probabilities based on its history. If P_s could not satisfy P_r during the latest request, then P_r should set π_B higher than π_G and decrease the value of $b_G(1)$.

Algorithm 1 is the process to select the most suitable serving peer using HMM. A requesting peer first establishes HMM for each selectable peer and then chooses the one with the largest $P(O|\lambda)$ as the serving node. When P_r requests the streaming service, P_r will execute the algorithm for the first time. Then during streaming, when the streaming quality of P_r declines to a predefined threshold, P_r will re-execute the selection algorithm and adapt parameters of each HMM.

```

1: procedure SELECT
2:    $N \leftarrow 2$ 
3:    $K \leftarrow \{0, 1\}$ 
4:    $O \leftarrow \{1\}$  with  $|O|$  random size
5:   for all  $P_s \in S(P_r)$  do
6:      $a_{BB} = a_{GB} = \frac{|C_{P_r}|}{|Neighbors_{P_s}|}$ 
7:      $b_G(1) = \text{Random}(0.5, 1)$ 
8:      $b_B(1) = \text{Random}(0, 0.5)$ 
9:      $\pi_B = 0.5$ 
10:    if  $P_s$  can't deliver data to  $P_r$  latest request then
11:      increase  $a_{BB}$  and  $a_{GB}$ 
12:      decrease  $b_G(1)$ 
13:      increase  $\pi_B$ 
14:    end if
15:     $a_{GG} = a_{BG} = 1 - a_{BB}$ 
16:     $b_G(0) = 1 - b_G(1)$ 
17:     $b_B(0) = 1 - b_B(1)$ 
18:     $\pi_G = 1 - \pi_B$ 
19:     $A \leftarrow \{a_{BB}, a_{GB}, a_{GG}, a_{BG}\}$ 
20:     $B \leftarrow \{b_G(1), b_G(0), b_B(1), b_B(0)\}$ 
21:     $\pi \leftarrow \{\pi_G, \pi_B\}$ 
22:     $\lambda_{P_s} \leftarrow \text{HMM}(N, A, B, K, \pi)$ ;
23:  end for
24:  select  $\lambda_{P_s}$  with maximum  $P(O|\lambda_{P_s})$ 
25:  return  $P_s$ 
26: end procedure

```

Algorithm 1. Peer Selection Using HMM

4 Evaluation

To investigate the performance of the proposed streaming model, we have carried out extensive simulations under various scenarios and the detailed experimental results are presented in this section. For each experiment, we report the mean value of results

obtained through 10 runs with different network size: 10^4 , 5×10^4 , 10^5 and 2×10^5 respectively. Peers belong to one of following layers 1, 2, 3, 4, 5 and the distribution is of uniform distribution. To quantify the performance of media streaming system, we define the streaming quality of a peer as

$$Q = \frac{\sum_{i=0}^{\kappa-1} Z_i}{\kappa} \quad (1)$$

where κ is the number of segments of a media content and Z_i is a variable that takes value 1 if segment i arrives at the receiver before its scheduled playback time, and 0 otherwise. Thus value of Q would range from 0 to 1, where 1 is the best streaming quality and 0 is the poorest one.

To compare the performance with our HMM streaming model, additional two methods of peer selection are presented here. The first one is called OPT algorithm. When performing peer selection using the OPT algorithm, P_r probes the status of bandwidth of each selectable peer before selecting peer. Then P_r selects senders that are probed and their bandwidth would be at least larger than P_r 's desired bandwidth, based on the collected information. It is obvious that such strategy would result in the best streaming quality since each requesting peer would have the up to date information of each selectable peer. However, OPT algorithm might suffered from heavily communication overhead. The second method to be compared with called Random algorithm, in which P_r selects senders from its selectable peer set randomly.

In the first simulation, streaming qualities of these three algorithms are compared. Figure 1 shows the compared results. OPT algorithm gets the best streaming quality. The quality of our algorithms is about 80% on average. In addition to its superior streaming quality, it can be shown that our algorithm is also scalable when the network size increases. Because Random algorithm selects peers in a random fashion without based on any information, it has the poorest streaming quality. In the second simulation, we examine overhead of these three algorithms. Figure 2 shows the compared results of communication overhead. By overhead, it means that how many requests (or probing message) a requesting peer would issue during streaming. It also indicates that how accurate a selection algorithm would select a suitable peer. The lower the value, the more accurate the algorithm is, since such algorithm would have had selected the most suitable peer for requesting peers. As shown in Figure 2, the HMM streaming algorithm has the lowest overhead. And its overhead is also scalable as the network size is increasing.

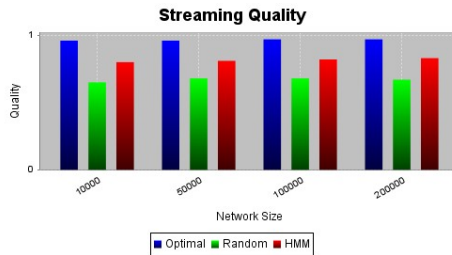


Fig. 1. Compared streaming quality with different selection methods

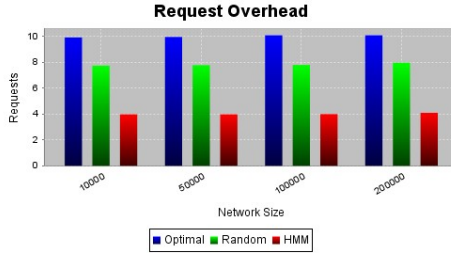


Fig. 2. Compared selection overhead with different selection methods

In the third simulation, we investigate differences of quality among different layers using the HMM streaming algorithm. Figure 3 shows the compared result among five layers. As shown from the result, the highest layer, the fifth layer, has the highest streaming quality and the lowest layer, the first layer, has the lowest quality on average. Such expectable result comes from that a priority mechanism is applied in the HMM streaming algorithm. It also shows that the proposed algorithm is endowed with fairness, since the more bandwidth offered to the network, the higher streaming quality would be obtained. The fourth simulation examines the impact of neighbors size using HMM streaming algorithm. Figure 4 shows the compared result of different neighbors size. Two different neighbors size are compared, namely 3% of the network size and 10% of the network size and the network size is of 10^5 peers. The size of neighbors affect how many selectable peers P_r would examine when performing algorithm, i.e. how many HMMs would be calculate. As shown from the result, larger size of neighbors would result in a better streaming quality since there are larger HMMs would be examined and would provide a more precise selection. However, larger HMMs would contribute considerable computations when calculating observation probability.

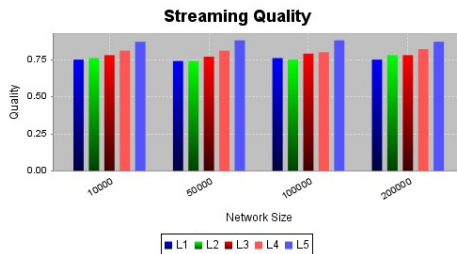


Fig. 3. Compared streaming quality with different layers using HMM streaming

In the fifth simulation, we show the robustness of our approach when peer failures occur frequently. Figure 5 presents the compared result of different ratios of peer failure. When there is no failure in the network, the average streaming quality is the highest among all others. However, under the situation that peer failures are possible, the streaming qualities of different failure ratios are still stable figures. Such results come

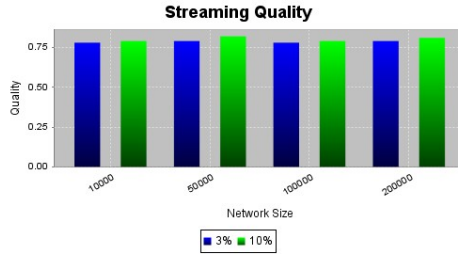


Fig. 4. Compact of neighbors size using HMM streaming

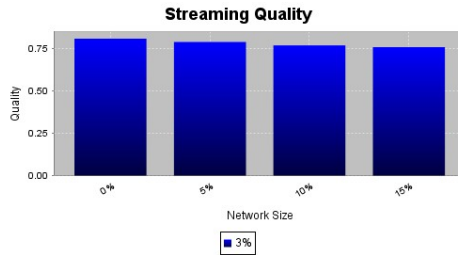


Fig. 5. Robustness of the HMM streaming model

from that when a requesting peer detect that a sender can't supply data anymore, the requesting peer would decrease $b_G(1)$ and increase a_{BB} , a_{GB} and π_B of this sender, that would made this sender less chance to be selected when the requesting peer perform peer selection next time. Therefore, our approach is robust under the situation where peers may fail frequently.

5 Related Work

There are two possible mechanisms when mentioning layered media streaming, namely cumulative streaming and noncumulative streaming [15]. In this paper, we adopt the cumulative layering approach in which the media data is encoded into one base layer and one or more enhancement layers. The base layer can be decoded independently, but enhancement layers are decoded cumulatively such that layer k can only be decoded when the layer 1 to the layer $k-1$ are decoded. In a non-cumulative streaming case, each layer is independent and the peer needs only subscribe to one layer. Peers in [16] decide which layers to request according to conditions on congestion and on spare capacity. PALS [17] allows requesting peers to orchestrate coordinated delivery by monitoring the overall throughput and periodically determining what is the target overall quality that can be delivered from all sending peers. K. Nahrstedt et al. [14] introduce requesting times of peers to determining a set of qualified sending peers for a requesting peer.

Other possible solutions to address the problem of peer-to-peer media streaming are by organizing network into structured hierarchical, one of them is called application

level multicast(ALM). In an ALM-based streaming system, a multicast tree is constructed for media delivering over the network. Such multicast tree solves the peers selection in the sense that the requesting-sending relations are defined by the child-parent relations. However, how to build and maintain a multicast tree efficiently and with scalable control overhead is a critical issue. Nice [12] and Zigzag [11] both adopt hierarchical distribution trees in which peers are organized in a hierarchy of bounded size clusters but are fundamentally different due to their own multicast tree construction and maintenance strategies. SpreadIt [7] builds a single distribution tree in which a joining process is done by traversing the tree nodes downward from the source until reaching a node that is unsaturated and could accommodate the request. A deleting process is performed with a redirect process while a child detects the parent failure.

Three possible solutions to the peers selection are based on offered bandwidth of peers and take into account of network condition. B. Bhargava. et al. [2] proposes an optimal media data assignment algorithm which leads to the minimum buffering delay for a requesting peer. In their works, peers are classified into N classes according to the N possible values of their offered bandwidth to the network and data assignment is done under considering the available set of sending peer and the buffered size. B. Bhargava et al. [8] studies three possible peers selection techniques, namely random, end-to-end, and topology-aware with different goodness estimations for sending peers.

6 Conclusion

In this paper, we study the problem of peer selection and solve the problem using HMM based a layered streaming model. Simulation results show that our algorithm can obtain a superior streaming quality. Our algorithm is also endowed with fairness and scalability, these being important characteristics of peer to peer streaming. The fairness comes from the feature that the more bandwidth a peer contributes to the network, the higher streaming quality this peer will obtain. And the scalability comes from the fact that the streaming quality also remains at a superior level as the network size is increasing. The contributions of our work are:

- We present an HMM streaming model to solve the peer selection problem and define parameters of HMM to model the status of bandwidth.
- Our method is distributed and is with scalability and fairness, which are all important factor to a distributed network.
- High streaming quality would be obtained when using the HMM streaming model and only small communication cost is introduced by our method.

In our approach, however, each peer is simply classified into two states, namely *GOOD* and *BAD*, which is prone for P_r to misjudge a peer's state. In our future work, we will model states of peers as multi-states in order to get an exact prediction of bandwidth usage. And we will also find a statistic model to define the observation symbol probability distribution rather than rely on a random behavior. In addition to defining the initial values of parameters of HMM more precisely, we will also develop an algorithm to re-estimate these parameters when the issued request is failed to be satisfied in our future work.

References

1. Rabiner, L.R.: A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. *Proceedings of the IEEE* 77(2), 257–286 (1989)
2. Xu, D., Hefeeda, M., Hambrusch, S., Bhargava, B.: On peer-to-peer media streaming. In: *Proc. of IEEE ICDCS 2002*, Vienna, Austria (2002)
3. Ganesh, A.J., Kermarrec, A.-M., Massouli, L.: Peer-to-Peer Membership Management for Gossip-Based Protocols. *IEEE Transactions on Computers* 52(2), 139–149 (2003)
4. <http://www.skype.com/>
5. Zheng, C., Shen, G., Li, S.: Distributed Prefetching Scheme for Random Seek Support in Peer to Peer Streaming Applications. In: *Proc. ACM P2PMMS 2005* (2005)
6. Wu, C., Li, B.: Peer-to-peer tree construction: Optimal peer selection for minimum-delay peer-to-peer streaming with rateless codes. In: *Proc. ACM P2PMMS 2005* (2005)
7. Castro, M., Druschel, P., Kermarrec, A.-M., Nandi, A., Rowstron, A., Singh, A.: SplitStream: high-bandwidth multicast in cooperative environments. In: *Proceedings of the nineteenth ACM symposium on Operating systems principles*, Bolton Landing, NY, USA (October 19–22, 2003)
8. Hefeeda, M., Habib, A., Botev, B., Xu, D., Bhargava, B.: PROMISE: Peer-to-Peer Media Streaming Using CollectCast. In: *Proc. of ACM Multimedia 2003* (2003)
9. Habib, A., Chuang, J.: Incentive Mechanism for Peer-to-Peer Media streaming. In: *Quality of Service, IWQOS 2004*. Twelfth IEEE International Workshop, June 7–9, pp. 171–180 (2004)
10. Zhang, M., Zhao, L., Tang, Y., Luo, J.-G., Yang, S.-Q.: Large-Scale Live Media Streaming over Peer-to-Peer Networks through Global Internet. In: *Proc. of ACM P2PMMS 2005* (2005)
11. Tran, D.A., Hua, K.A., Do, T.: ZIGZAG: An Efficient Peer-to-Peer Scheme for Media Streaming. In: *Proc. of IEEE INFOCOM 2003* (2003)
12. Banerjee, S., Bhattacharjee, B., Kommareddy, C.: Scalable Application Layer Multicast. In: *Proc. of ACM SIGCOMM 2002* (2002)
13. Deshpande, H., Bawa, M., Garcia-Molina, H.: Streaming Live Media over a Peer-to-Peer Network. Technical report, Stanford Database Group 2001–20 (August 2001)
14. Cui, Y., Nahrstedt, K.: Layered peer-to-peer streaming. In: *Proc. of ACM NOSSDAV* (2003)
15. Kim, T., Ammar, M.: A comparison of layering and stream replication video multicast scheme. In: *NOSSDAV. International Workshop on Network and Operating Systems Support for Digital Audio and Video* (2001)
16. McCanne, S., Jacobson, V., Vetterli, M.: Receiver-driven layered multicast. In: *ACM SIGCOMM* (1996)
17. Rejaie, R., Ortega, A.: PALS: Peer to peer adaptive layered streaming. In: *NOSSDAV* (June 2003)

Optimum Power Controller for Random Number Generator in the Crypto Module of Ubiquitous Computing Environment

Jinkeun Hong¹ and Kihong Kim²

¹ Division of Information & Communication Engineering, Baekseok University
115, Anseo-dong, Cheonan-si, Chungnam, 330-704, South Korea

jkhong@bu.ac.kr

² Network & Communication Security Division, ETRI
P.O. Box 1, Yuseong, Daejeon, 305-600, South Korea

hong0612@hanmir.com

Abstract. Critical cryptography applications require the production of an unpredictable and unbiased stream of binary data derived from a fundamental noise mechanism, which is quite difficult to create with a stable random bit stream, as required for statistical randomness, when using a random generator with only a hardware component. However, since all electronic systems are influenced by a finite bandwidth, $1/f$ noise, and other non-random influences, perfect randomness cannot be preserved by any practical system. Thus, when generating random numbers using an electronic circuit, a low-power white noise signal is amplified, then sampled at a constant sampling frequency. Yet, it is quite difficult to create an unbiased and stable random bit stream, as required for statistical randomness, when using a random generator with only a hardware component and in especially it has occur the drift phenomena of input power. Therefore if the randomness of output bit stream is beyond limits range, it is applied the regulation of input power range to take the output bit stream, through the evaluation of randomness by constant period of output bit stream. Accordingly, this paper proposes a method for stabilizing the input power of a random number generator using optimum power control mechanism in crypto module hardware. As such, the proposed scheme is designed to reduce the statistical property of a biased bit stream and optimize the input power to a random number generator engine in crypto module engine for ubiquitous computing.

1 Introduction

In recent years, ubiquitous computing advocates the construction of massively distributed computing environments that consumer electronics, sensors, global positioning system (GPS) receives. Bluetooth originally thought of as a “serial cable replacement” for small computer peripherals, and 802.11, originally developed as a wireless LAN system for mobile devices (laptop, PDA) [1] [2] [3]. In this environment, ubiquitous computing imposes peculiar constraints computational

power and energy budget, which make this case significantly different from those contemplated by the canonical doctrine of security in distributed systems. There are many security issues in the ubiquitous environment, including authentication, authorization, accessibility, confidentiality, integrity, and non repudiation. And other issues include convenience, speed, and so on. A H/W random number generator uses a non-deterministic source to produce randomness, and more demanding random number applications, such as cryptography, smart card crypto engine, and statistical simulation, benefit from sequences produced by a random number generator, a cryptographic system based on a hardware component [1]. As such, a number generator is a source of unpredictable, irreproducible, and statistically random stream sequences, and a popular method for generating random numbers using a natural phenomenon is the electronic amplification and sampling of a thermal or Gaussian noise signal.

However, since all electronic systems are influenced by a finite bandwidth, $1/f$ noise, and other non-random influences, perfect randomness cannot be preserved by any practical system. Thus, when generating random numbers using an electronic circuit, a low-power white noise signal is amplified, then sampled at a constant sampling frequency. Yet, it is quite difficult to create an unbiased and stable random bit stream, as required for statistical randomness, when using a random generator with only a hardware component. The studies reported in [2] [3] [4] show that the randomness of a random stream can be enhanced when combining a real random number generator, LFSR number generator, and hash function. However, the randomness of this combined method is still dependent on the security level of the hash function and LFSR number generator.

Therefore, controlling a stable input voltage for a random number generator is an important aspect of the design of a random number generator. In previous studies, Peiris and Annakkage examined the use of logic modulation for damping power system oscillations [5], while Zang and Phillis proposed the use of logic to solve the admission control problem in two simple series paralleled networks [6]. Plus, logic has also been applied to admission control in communication networks [8]. If it is occurred the transition of input power due to circumstance effects, temperature, transition of time, it is not guaranteed the stable output bit stream and the randomness of randomness number generator output bit stream is not guaranteed. Therefore when it is occurred the drift of input power deviation, it is needed to design the mechanism, which can be guaranteed the randomness of output bit stream. Accordingly, this paper proposes a optimum power approach to ensuring a stable input power for a random number generator engine. The stability of the input power is a very important factor in the randomness of a random number generator engine. Thus, to consistently guarantee the randomness of an output sequence from a random number generator, the origin must be stabilized, regardless of any change of circumstance elements. Therefore, a random number generator is proposed that applies power logic control, thereby providing the best input power supply. Additionally we use measure of randomness test to decide DB base and its measure is provided

the efficiency, which is fast and not weighty due to use test bits of 200,000bits, when it is evaluated the randomness of output stream.

Hereinafter, section 2 reviews the framework of power logic control. Then, section 3 examines a case study, experimental results and some final conclusions are given in section 4.

2 Framework of Optimum Power Controller (OPC) in Crypto Module

Most crypto module microcomputer chips are consists of CPU, ROM, RAM, I/O, EEPROM, etc. The ROM contains the chip operating system and the RAM is the process's working memory.

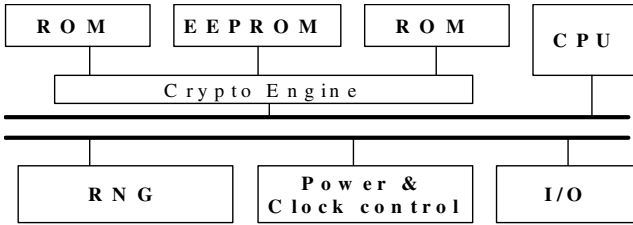


Fig. 1. Microcomputer architecture of crypto module

In the EEPROM memory, data and program can be written to and read from the EEPROM under the control of OS. Within the card, data are passed through a bus under the security logic's control. Crypto module has some form of power and clock control circuitry, BUS, and I/O interface.

The H/W random number generator includes common components for producing random bit streams, classified as follows: characteristics of the noise source, amplification of the noise source, and sampling for gathering the comparator output [10] [11]. The applied noise source uses Gaussian noise, which typically results from the flow of electrons through a highly charged field, such as a semiconductor junction [12] [13] [14] [15].

Ultimately, the electron flow is the movement of discrete charges, and the mean flow rate is surrounded by a distribution related to the launch time and momentum of the individual charge carriers entering the charged field. The Gaussian noise generated in a PN junction has the same mathematical form as that of a temperature-limited vacuum diode. The noise seems to be generated by the noise current generator in parallel with the dynamic resistance of the diode. The probability density $f(x)$ of the Gaussian noise voltage distribution function is defined by Eq. (1).

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} \quad (1)$$

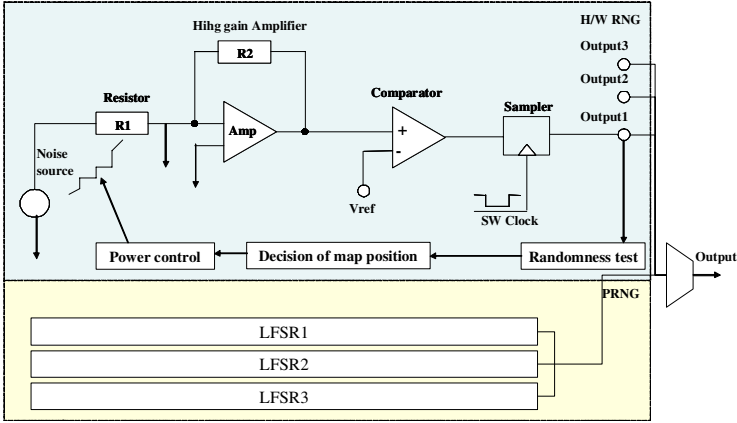


Fig. 2. RNG (H/W RNG & PRNG) module architecture

Here, σ is the root mean square value of Gaussian noise voltage. However, for designed Gaussian noise random number generator, the noise diode is used the diode with white Gaussian distribution. The power density for noise is constant with frequency from 0.1Hz to 10MHz and the amplitude has a Gaussian distribution. $V_n(rms)$ is the *rms* value of noise standard deviation of distribution function. The noise must be amplified to a level where it can be accurately thresholded with no bias by a clocked comparator. Although the *rms* value for noise is well defined, the instantaneous amplitude of noise has a Gaussian normal distribution.

$$V_n(rms) = \sqrt{4kTRB} \tag{2}$$

Here, k is Boltzmann constant ($1.38 \times 10^{-23} J/deg.K$), T is absolute temperature (deg. Kelvin), B is noise bandwidth (Hz), R is resistor (ohms). If $4kT$ is 1.66×10^{20} and R is $1K$, B is $1Hz$, then $V_n(rms) = \sqrt{4kTRB} = 4nV/\sqrt{Hz}$. The applied voltage is $15Vdc$, and current limiting resistor is $16k\Omega$. Noise comes from agitation of electrons within a resistance, and it sets a lower limit on the noise present in a circuit. When the frequency range is given, the voltage of noise is decided by a factor of frequency. The crest factor of a waveform is defined as the ratio of the peak to the *rms* value. A crest value of approximately 4 is used for noise.

However, for the proposed real random number generator, the noise diode is a noise diode with a white Gaussian distribution. The noise must be amplified to a level where it can be accurately thresholded with no bias using a clocked comparator.

This section provides a short description of the framework of a FLC [5] [6] [7] [8] as follows: the input power source (1), generate engine that generates random numbers (2), random test process (3), decision of voltage map position (4), DB map table (5), and regulation of power control (6). The proposed optimum

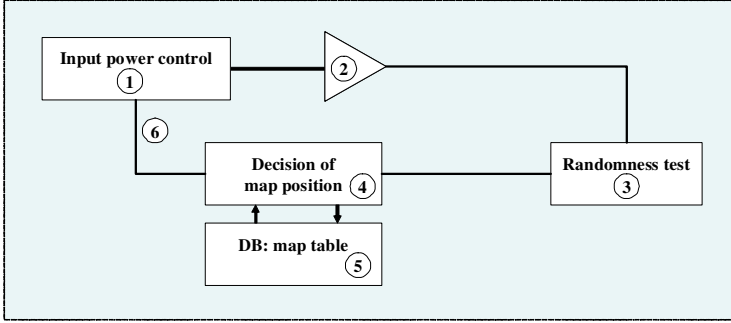


Fig. 3. Optimum power control framework used to generate random numbers

power control framework is consists of three components, such as decision of map position, and management of voltage map table.

- *Generate engine that generates random numbers and randomness test block:* A generating engine that generates random numbers includes common components for producing random bit streams. It can be characterized as encompassing the following: A Gaussian noise process, a source amplification process, and a sampling process [10] [11]. The cryptographic modules that implement a random number generator engine also incorporate the capability to perform statistical tests for randomness.
- *Decision of map position, management of voltage map table:* To set up the position of a voltage map, a map DB is managed, and the parameters in the map DB consist of the current VP value, the LST VP, the DVP, the lower bound value, and the upper bound value, as shown in Table 1.

Table 1. Voltage map table to decide voltage position

| Parameter | Current VP | LST VP | DVP | Lower bound | Upper bound |
|-----------|------------|-----------|--------|-------------|-------------|
| Voltage | V_c | V_{lst} | + or - | V_D | V_U |

Here, VP is voltage point value, $LST VP$ is the last voltage point value, and DVP is the direction value of the voltage point. The current VP is set at V_c , and the decision voltage value, $LST VP$, is set at V_{lst} after the test evaluation of the last randomness of the output bit stream. If it is increased to the value of $LST VP$, then the value of DVP is positive, and the last decision value V_{lst} is increased in reference of the current $VP V_c$, as shown in Eq. (3) and Fig. 4. Here, ΔV is an acceptable level of voltage for voltage regulation.

$$V_{lst} = V_c + (DVP)\Delta V \tag{3}$$

In Fig. 4 to decide at the point of the optimum time controlled interval, the threshold level is set up and V_c at the current time point t_i , V_{lst} at the next time

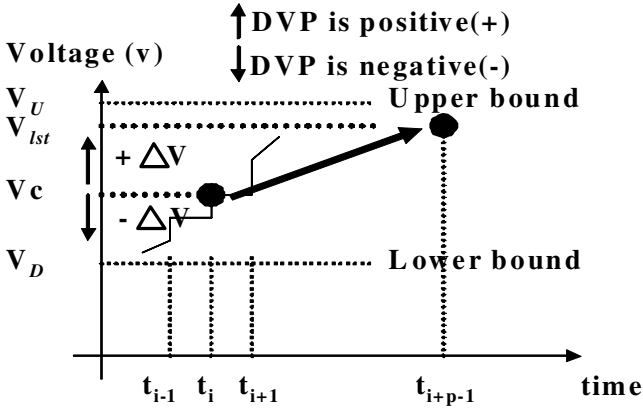


Fig. 4. Optimum power control setting process of output bit stream

point t_{i+p-1} results. In Fig. 5, when the randomness of the output bit stream is evaluated, if it is found to deviate from the threshold level of randomness, then it is considered as a failed region during the period of time interval T_p . The value of the count is summed, and if it is more than that of threshold level, the optimum power control can be operated.

$$E_p = \{E_{i-1}, E_i, E_{i+1}, \dots, E_{i+p-1}\} \tag{4}$$

Here, i is $1, 2, 3, \dots, n$, and E is the result of the randomness evaluation test during the each period time (T_p).

$$T_p = \{t_{i-1}, t_i, t_{i+1}, \dots, t_{i+p-1}\} \tag{5}$$

In addition, δ is a decision factor; it is also a threshold level and reference condition that is used for verifying the success rate of the randomness factor.

The OPC algorithm evaluates the randomness test for the output bit stream after the interval of the period T_p . When the iteration result of the randomness evaluation is greater than the value of the threshold level, then the regulation of the input power level is determined and the optimum power control process is controlled as follows:

Each of the following random number tests is implemented to test a sequence length of 200,000 bits. In Fig. 6 the frequency test determines whether the number of ones and zeros in a sequence approximate the number expected for a truly random sequence.

The upper bound value of the threshold level is not greater than 3.841. The serial test is the frequency of each and every overlapping m bit pattern; this is used to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (m and $m + 1$) against the expected result for a random sequence. In this case, the value of the threshold level is under the outer bound of 5.991. A poker test is used to divide the sequence into k non-overlapping m length sequences.

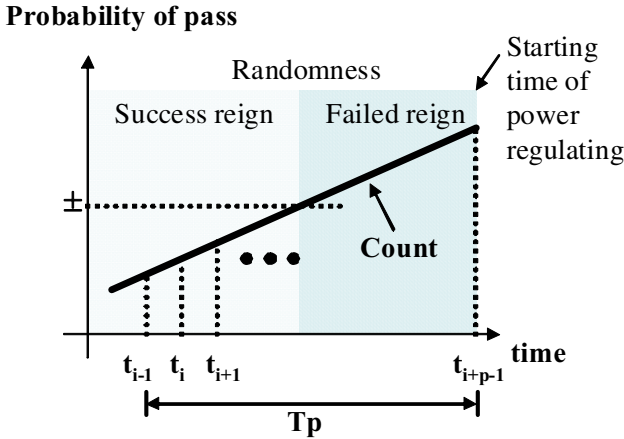


Fig. 5. Setting up of optimum power control time

The value of the threshold level is under 14.067 for a length of 3. These sequences are compared to a 2^m space, and with each match the value total increases. An autocorrelation test checks for the correlation between the current sequence and the shifted sequence. The value of the threshold level is under 0.05.

3 Experimental Results

The decision of the optimum power map position is converted by a value based on a DB map table. When the input power remains within the border area, the output random number sequence maintains stable randomness. When five levels of input power are given, the randomness of the output random number sequences is as shown in Table 2.

The randomness of the output random number sequence reacted sensitively whenever the input power supply was changed. Therefore, the experimental model was shown to highlight the relationship between the randomness and variations in the input power, where the randomness of the output random number sequences was found to depend on the input power, and a threshold value could be used to determine the randomness of the output random number sequence engine. Therefore, modifications in the input power controlled by the proposed OPC were used to stabilize this interdependence between the input power and the randomness of the output random number sequences. In Table 3, the initial input power was set between 9.6V and 10.4V, and the result of the randomness evaluation passes in a given time interval. After a lapse of a specific time, due to the drift of the surrounding conditions, such as drift of the input power level or in the specific circuitry, the randomness security level of output bit stream is not always guaranteed in the case of a generally stable designed input power range condition.

If the result of the randomness evaluation passes at a level of 90% with a generated random number speed 200kbps and a 1 day T_p value, the number of

Algorithm: process of optimum power control

Optimum_Controller() ::

1. Let threshold level of randomness γ ;
2. Given RNGSequence size: $w = i \times 200000, i = \{0, \dots, n\}$;
3. for $i = \{0, \dots, n\}$ times do
4. Result = EvaluationTest(w);
5. if (Result == 'False') then count++;
6. if (count > δ) then Regulate_Power_Control();
6. End for

Evaluation_Randomness(width) ::

1. width {
2. If $\|D\| \leq \delta$, then D[width] is PassBitStream, SaveBit Stream=D[width], return 'True';
3. Else, D[width] is discarded, return 'False'; }

Regulate_Power_Control()::

1. DB_map_check: $V_c, V_{ist}, V_U, V_D, DVP$;
2. Check randomness of controller output stream after regulation voltage according to DB map value;
3. Decision of V_{ist} to the direction value DVP(+: increased direction, -: decreased direction);

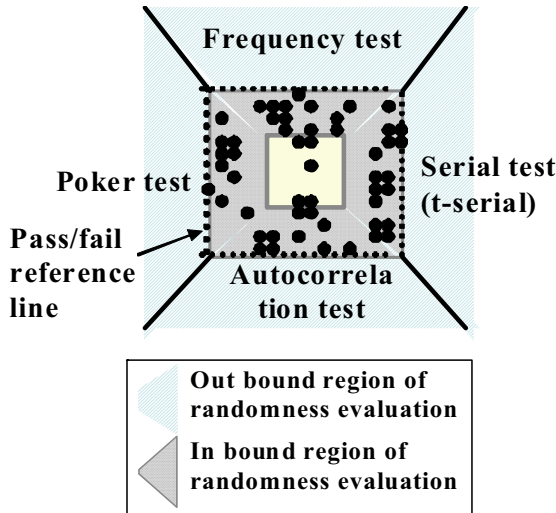


Fig. 6. Bound lines in the randomness evaluation of output bit streams

Table 2. Relationship between the result of randomness test and input power

| Voltage | 9.65V | 9.83V | 10.0V | 10.15V | 10.3V |
|---|--------------|--------------|--------------|--------------|--------------|
| Pocker test (block=4) ($X < 24.9$) | 7.8 PASS | 12.1 PASS | 13.0 PASS | 21.5 PASS | 15.7 PASS |
| Pocker test (block=5) ($X < 44.7$) | 28.6 PASS | 41.2 PASS | 30.5 PASS | 44.0 PASS | 24.1 PASS |
| t-serial test (block=4) ($X < 15.5$) | 4.1 PASS | 5.0 PASS | 11.4 PASS | 4.8 PASS | 4.8 PASS |
| t-serial test (block=5) ($X < 26.3$) | 16.3 PASS | 23.3 PASS | 18.9 PASS | 26.4 PASS | 22.5 PASS |

Table 3. The pass/fail condition according to tolerant input power range in general case

| Voltage | $V_{lst} < 9.6V$ | $9.6V < V_{lst} < 10.4$ | $V_{lst} > 10.4$ |
|----------------------|------------------|-------------------------|------------------|
| Frequency test | Fail | Pass | Fail |
| Serial test | Fail | Pass | Fail |
| t-serial test | Fail | Pass | Fail |
| Pocker test | Fail | Pass | Fail |
| Autocorrelation test | Fail | Pass | Fail |

collected bit streams that pass the randomness evaluation is 1.56×10^{10} bits. Additionally, the number of discarded bit streams that fail is 1.73×10^9 bits. The condition of T_p is set at 1 hour with the OPC; the number of collected bit streams is 6.48×10^8 bits and the number of discarded bit streams is 7.2×10^7 bits.

Otherwise if the OPC is not applied, the output bit stream of the random number generator cannot guarantee randomness. In Table 5, although the pass probability is degraded at 80% due to the state of random number generator, if the RNG is applied with the OPC, a guaranteed 1.56×10^{10} bits will be determined, which is at least 90%. If the OPC is not applied, the result is then a guaranteed 1.38×10^{10} bits, approximately. If the management of the random number generator is neglected, the pass probability of the output bit stream is degraded, and the security characteristics and stability of the random number generator can no longer be guaranteed.

In Fig. 7, the collected bits are compared with the OPC and without OPC. Here, the randomness level is satisfied, in terms of a variable T_p , such as a variable pass probability.

If the T_p value is 1 day, although the degradation of the random number generator occurs, indicating that the pass probability has been degraded, and if the OPC is applied, it can be guaranteed that a stable and secure output bit stream will function continuously. Otherwise, if the OPC is not adopted, as in the degradation state of the random number generator, the collected number of guaranteed bit streams is reduced, which satisfies the randomness condition.

Table 4. Pass/fail bits in condition of 200kbps/2Mbps (pass rate = 90%)

| T_p | 200kbps | 200kbps | 2Mbps | 2Mbps |
|-------|-----------------------|--------------------|-----------------------|-----------------------|
| | Pass bits | Fail bits | Pass bits | Fail bits |
| 1sec | 1.8×10^5 | 2.0×10^4 | 1.8×10^6 | 2.0×10^5 |
| 10min | 1.08×10^8 | 1.2×10^7 | 1.08×10^9 | 1.2×10^8 |
| 1hrs | 6.48×10^8 | 7.2×10^7 | 6.48×10^9 | 7.2×10^8 |
| 1day | 1.56×10^{10} | 1.73×10^9 | 1.56×10^{11} | 1.73×10^{10} |

Table 5. Pass/fail bits in condition of 200kbps (pass rate = 80%)

| T_p | Without OPC | Without OPC | With OPC | With OPC |
|-------|-----------------------|--------------------|-----------------------|--------------------|
| | Pass bits | Fail bits | Pass bits | Fail bits |
| 1sec | 1.6×10^5 | 4.0×10^4 | 1.8×10^5 | 2.0×10^4 |
| 10min | 9.6×10^7 | 2.4×10^7 | 1.08×10^8 | 1.2×10^7 |
| 1hrs | 5.76×10^8 | 1.44×10^8 | 6.48×10^8 | 7.2×10^7 |
| 1day | 1.38×10^{10} | 3.46×10^9 | 1.56×10^{10} | 1.73×10^9 |

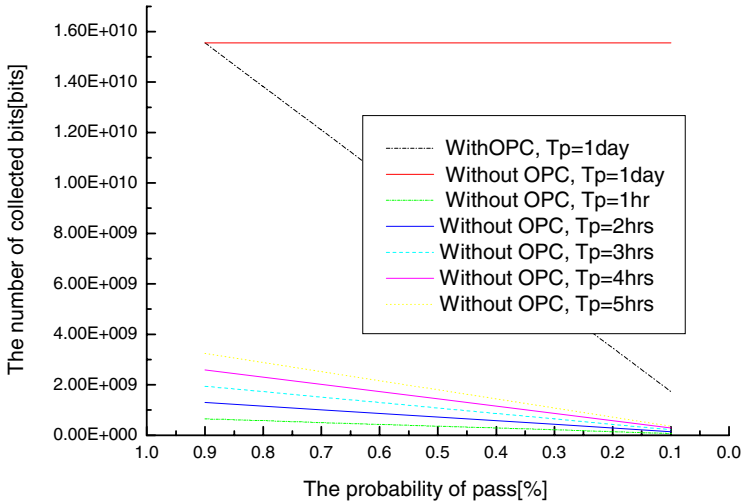


Fig. 7. Bound lines in the randomness evaluation of output bit streams

Moreover, if the period of the test interval T_p becomes short enough, the time consumed during the test of randomness is enhanced and the period for the detection rate is short. Otherwise, if the period of the test interval is relatively long, the time consumed for the test of the randomness is reduced. However, if the state of the random number generator fails due to the drift of input power, the generated bits stream during the interval must be discarded. Therefore, it is necessary to study the optimum power control in addition to the related period.

4 Conclusion

In ubiquitous computing, a smart card consists of a chip and an integral operating system. The chip contains the CPU, ROM, RAM, I/O functions, and the EEPROM. Some smart card microprocessors use a RNG and cryptographic processors. An optimum power controller was proposed and applied to the input power of a random number generator engine in crypto-processor of crypto module. A random number generator uses a non-deterministic source to produce randomness, and more demanding random number applications, such as cryptography and statistical simulation, benefit from sequences produced by a random number generator, a cryptographic system based on a hardware component in a smart card. Nevertheless, the stability of the input power is very important in ensuring the randomness of a random number generator engine. Therefore, to guarantee the randomness of the output sequences from a random number generator consistently, a method that can stabilize the origin quickly, regardless of any changes in the circumstance elements, is presented. Tests showed that the proposed optimum power controller using a length of 200,000bits is effective and rapid in stabilizing the input power of a random number generator engine in a crypto module.

References

1. Alireza, H., Ingrid, V.: High-Throughput Programmable Crypto-Coprocessor. IEEE Computer Society, Los Alamitos (2004)
2. Jalal, A.M., Anand, R., Roy, C., Dept, M.D.: Cerberus: A Context-Aware Security Scheme for Smart Spaces. In: IEEE PerCom 2003 (2003)
3. Attoh-Okine, N.O., Shen, L.D.: Security Issues of Emerging Smart Cards Fare Collection Application in Mass Transit (1995)
4. WiTness: Interaction of SIM based WiTness Security Functions and Security Properties of Mobile Devices and Communication Channels, Information society (2003)
5. Peiris, H.J.C., Annakkage, U.D., Pahalawaththa, N.C.: Generation of Fuzzy Rules to Develop Fuzzy Logic Modulation Controllers for Damping of Power System Oscillations. IEEE Trans. on Power System 14(4) (1999)
6. Zang, R., Phillis, Y.A.: Admission Control and Scheduling in Simple Series Paralleled Networks Using Fuzzy Logic. IEEE Trans. on Fuzzy Systems 9(2) (2001)
7. Klir, G.J., Yuan, B.: Fuzzy Sets and Fuzzy Logic Theory and Applications. Prentice-Hall International Inc., Englewood Cliffs (1995)
8. Le, Q., Knapp, G.M.: Incorporating Fuzzy Logic Admission Control in Simulation Models. In: Winter Simulation Conference (2003)
9. Kimberley, M.: Comparison of Two Statistical Tests for Keystream Sequences. IEE Electronics Letters 23(8) (1987)
10. Petrie, C.S., Connelly, J.A.: A Noise-Based Random Bit Generator IC for Applications in Cryptography. In: ISCAS 1998 (1998)
11. Delgado-Restituto, M., Medeiro, F., Rodriguez-Vasquez, A.: Nonlinear Switched-Current CMOS IC for Random Signal Generation. IEE Electronic Letters 29 (1993)
12. <http://www.io.com/~ritter/RES/NOISE.HTM>
13. <http://www.clark.net/pub/cme/P1363/ranno.html>

14. http://webnz.com/robert/true_rng.html
15. Ya, B., Ryabko, Matchikina, E.: Fast and Efficient Construction of an Unbiased Random Sequence. IEEE Trans. on Information Theory 46(3) (2000)
16. Timothy Holman, W., Alvin Connelly, J., Dowlatabadi, A.B.: An Integrated Analog/Digital Random Noise Source. IEEE Trans. on Circuits and System I: Fundamental Theory and Applications 44(6) (1997)
17. FIPS 140-1: Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-1, U.S. Department of Commerce/NIST[National Technical Information Service] (1994)
18. <http://csrc.ncsl.nist.gov/fips/fips1401.htm>
19. <http://stat.fsu.edu/~geo/diehard.html>

Problem Localization for Automated System Management in Ubiquitous Computing*

Shunshan Piao, Jeongmin Park, and Eunseok Lee**

School of Information and Communication Engineering Sungkyunkwan University
300 Chunchun Jangahn Suwon, 400-746, Korea
{sspiao, jmpark, eslee}@ece.skku.ac.kr

Abstract. The increasing complexity of Ubiquitous computing leads to the challenges in managing systems in an automated way, which accurately identifies problems and solves them. Many Artificial Intelligent techniques are presented to support problem determination. In this paper, a mechanism for problem localization based on analyzing real-time streams of system performance for automated system management is proposed. We use Bayesian network to construct a compact network and provide both inductive and deductive inferences through probabilistic dependency analysis throughout the network. An algorithm for extracting a certain factors that are highly related to problems is introduced, which supports network learning in diverse domains. The approach enables us to both diagnose problems on the underlying system status and predict potential problems at run time via probabilities propagation throughout network. A demonstration focusing on system reliability in distributed system management is given to prove the availability of proposed mechanism, and thereby achieving self-managing capability.

Keywords: Fault Diagnosis, Prognosis, Problem Localization, Probabilistic Dependency Analysis, Self-Managing.

1 Introduction

With the rapid growth in size and flexibility in distributed computing systems nowadays, complexity appears frequently in all places especially in Ubiquitous Environment. Due to the fact that the more the requirements demanded, the more the complexities created [1], it brings much more burdens and hardness for administrators to handle abnormalities and maintain high system reliability, which is very important to system manager for managing the computer system and to users for running their applications. However, as autonomic computing [2] requirements emerged, self-managing ability appears on the IT stage as a challenging topic. It implies that the system can recover from faults on its own initiative instead of system administrators'

* This work was supported in parts by Ubiquitous Autonomic Computing and Network Project, 21th Century Frontier R&D Program, MIC, Korea, ITRC IITA-2006-(C1090-0603-0046), Grant No. R01-2006-000-10954-0, Basic Research Program of the Korea Science & Engineering Foundation, and the Post-BK21 Project.

** Corresponding author.

direct handling, for the purpose of providing services to maintain high reliability without interruptions. As faults are unavoidable in the whole lifecycle of computer systems, problem localization techniques [3] generates a variety of challenging applications for the Artificial Intelligent techniques to provide fault localization technology, root cause analysis and other approaches applied to the fields of problem analysis.

With current increasing complexity, knowledge of the system and environment is not sufficient as we need to analysis the exact cause of unexpected problems in large scale of distributed environment; so much as exceptions and abnormalities occur without any anticipation. Existing techniques such as rule-based or case-based algorithms are not competent. In some cases, it is not popular in uncertain domain with missing information and inferring with low accuracy, and it becomes large size as increasing states [4]. Moreover, most existing researches on analyzing causes of problems [5] focus on post-treatment, which means that dealing with problems is time consuming, error-prone, and requires much experience and prior information.

Problem localization is a process of deducing the exact root cause of problems based on a set of observed information. Clearly, it is critical to designing an effective self-managing system, by which the system determines and solves problems automatically. In this paper, we propose a mechanism for fault localization based on Bayesian machine learning method to determine the cause of problems and also enable it to forecast under given observations via probabilistic dependency analysis. We add preconditioning course before learning structure, which improves the efficiency of structure learning without degrading the quality of learning. Following the proposed approach in performance problem domain, bidirectional inferences including fault diagnosis and prognosis are possible to conduct automated system management in complex distributed system, and hence improve system reliability.

The rest of this paper is organized as follows. First, we provide related work on autonomic computing and list some problems in existing research, which focuses on fault diagnosis and fault management. Second, following the introduction of Bayesian network fundamental, we describe the proposed fault localization model structure in detail, then introduce preprocessing and structure learning. Third, we examine a straightforward application of learning network and discuss how to implement problem localization under the proposed approach. In the last section, we conclude this paper and provide directions for future research.

2 Related Works

Self-managing system tasks in Ubiquitous environment such as real-time fault localization and problem diagnosis, call for higher levels of automation. Many recent studies introduce various methods for automated system management [6], attempting to explore new approaches to improve self-managing capability, such as IBM self-aware distributed systems and Sun fault management in predictive self-healing.

- IBM Self-Aware Distributed Systems

IBM research on self-aware distributed systems aims at automating an increasingly complex and expensive task of real-time problem diagnosis in large-scale distributed system by using state-of-art machine learning - Bayesian inference, probabilistic

reasoning and information –theoretic approaches. It shows an architecture of diagnosis system called RAIL (Real-Time Active Inference and Learning), which uses the probe outcomes to make inferences about the system state, and actively requests the next most-informative probes to improve its diagnosis. [7]

The most current focus of the work is on:

- Active diagnosis: Adjusting the probe set dynamically to improve diagnosis;
- Extending local approximation techniques to incremental, real-time scenarios;
- Handling intermittent failures, dynamic routing, and other nonstationarity in the network state and behavior using on-line learning;
- Active learning using flexibility in probe selection.

- Sun Fault Management Utilities in Predictive Self-healing

The Sun Fire X4500 server features the latest fault management technologies. This technology is incorporated into both the hardware and software of the server. Predictive Self Healing introduces a new software architecture and methodology for fault detection, diagnostics, logging, and system service management across Sun's product line. There are two major components in Predictive Self Healing [8]: Fault Management Architecture (FMA) and Service Management Facility (SMF).

Predictive self healing addresses two problems of commercial IT:

- Fix problems before they occur
- Circumvent operational problems with services

A critical event prediction for proactive management describes an attempt to build a proactive prediction and control system for large clusters either through prediction algorithms or root cause solutions using probabilistic networks, including time-series, rule-based classification and Bayesian network models [1]. Furthermore, a hybrid prediction model in ubiquitous computing system adopts a selective model according to the system context, using various algorithms with respective characteristics, which can predict system situations before errors occur [4].

Various machine learning algorithms are used in the automated system management. However, most of them rarely consider dependency relationships between collected information. In the case of such a situation, with the fact that there exist somewhat interrelated relationships between system metrics, it can start with representing a probabilistic dependency model among system elements rather than deeming them mostly independent.

3 Problem Localization

A key essential of self-managing is the ability of the system to perform real-time inferences and learning about its own behavior, to diagnose and predict various problems and performance degradations, namely, the capability of self-awareness. "Suit the remedy to the case". Only with the root cause of a problem can we make the system take appropriate actions or repair strategies to solve the problem. Furthermore, adding proactive prediction ability makes it prevent from unexpected loss through pretreatment, and hence achieve automated system management. Fault diagnosis and prognosis based on real-time streams of computer events contribute to self-managing

for the purpose of determining root causes of problems i.e. fault localization and predicting future situations such as potential problems that going to occur.

In this paper, we use probabilistic machine learning method, which is mainly used as a modeling tool, to propose an inference model structure for fault diagnosis and prognosis in self-managing systems. It infers the likelihood that a factor is in one state which is dependent on other factors' states that reflect the degrees of confidence. In terms of accuracy and efficiency of diagnosing problems and forecasting potential problems, we can deal with the data in the raw beforehand then combine prior information for inference.

3.1 Proposed Model Structure

Bayesian network based problem localization model structure is described in Fig. 1.

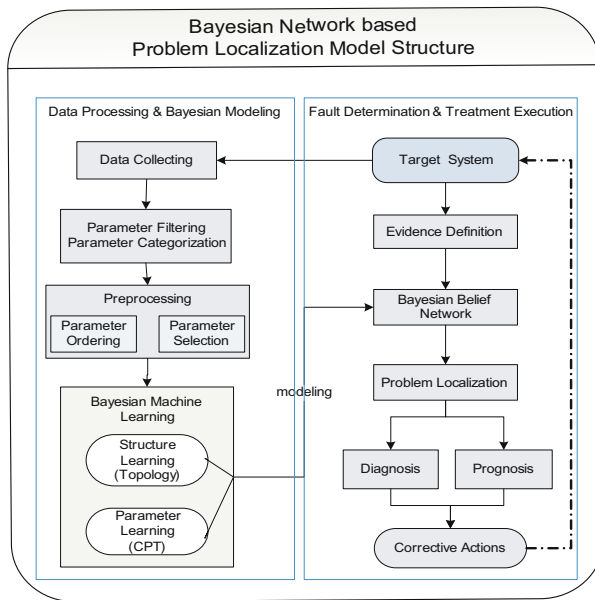


Fig. 1. Bayesian Network based Problem Localization Model Structure

- **Data Collecting:** System real-time performance data is collected which also includes the system health states stored in the log file from target system via monitoring.
- **Parameter Filtering & Categorization:** The dataset, collected from the system log file, consists of real-time continuous parameters which are then discretized.
- **Preprocessing:** This processing course, mainly affecting the ultimate inference, is processed before using a Bayesian network. Herein we propose an approach based using information theory among filtered parameters, select a certain parameters and rank them in a node list that will be applied in structure learning.
- **Bayesian Machine Learning for modeling Bayesian Belief network:** 1) **Topology Structure Learning:** It finds a network structure that is most probable matching to

the training data. 2) Parameter Learning: It decides on the conditional probability table of each node by learning from training data given a created network.

- Evidence Definition: This defines degree of confidence information which is called evidence by presenting with probabilities.
- Problem Localization including Diagnosis & Prognosis: Decided evidences are posted to constructed network to reason out $P(Cause | Effect)$ or $P(Effect | Cause)$ in different cases for determining high impact factor of faults or predicting potential problems under certain conditions.

The parameter with the highest probability in the network is determined as the cause after probability propagation when making inferences. According to inference results, corrective repairs are taken to running system in order to keep continuous operation without pause. Analyzing statistic data from a given system, we can find patterns of system without knowing the inner running mechanism and conduct inference based on this.

3.2 Fundamental and Characteristics of Bayesian Network

Bayesian network or Bayesian belief network is a graphical structure to represent and reason about an uncertain domain, including nodes represent random variables of interest in the domain and arcs represent direct influences i.e. conditional dependencies between variables. It emphasizes that a link between two nodes does not, and need not, always imply causality, i.e. the network is not always a causal structure. It only implies a direct influence of parent node over child node in the sense that the probability of child node is conditional on the value of parent node, and two nodes may have a link between them even if there is no direct cause [9]. The formula (1) expressed below is a simple representation of Bayes' rule.

$$P(A | B) = \frac{P(B | A) \cdot P(A)}{\sum_i P(B | A_i) \cdot P(A_i)} \tag{1}$$

For more complex problems, it also has a mechanism that can propagate probabilities via extending Bayes' Rule throughout the whole network automatically. If a Bayesian network encodes the true independence assumptions of a distribution, we can use a factored representation for the distribution as follows:

$$\begin{aligned} P(x_1, \dots, x_n) &= \prod_{i=1}^n P(x_i | x_{i+1}, \dots, x_n) \\ &= \prod_{i=1}^n P(x_i | Pa(x_i)) \end{aligned} \tag{2}$$

Formula (2) shows that instead of the full joint distribution, we need only the conditional probabilities of a variable given its parents, which is based on Markov assumption. A distinct characteristic of Bayesian network is that it is especially useful in uncertainty domains with information about the past and/or the current situation being vague, incomplete, and conflicting. It's easy to explain how a system arrived at a particular recommendation, decision, or action as it can represent probabilistic relationships between nodes dynamically. Furthermore, Bayesian Network can be run in multiple directions, including bottom-up and top-down, which features of Bayesian

Network are applied in this paper. Another feature is that it can post evidence to a Bayesian belief network to predict a result or to diagnose a cause based on analyzing current beliefs. The evidence is information about a current situation and beliefs are the probability that a variable will be in a certain state based on the addition of evidence in a current situation [10].

3.3 Preprocessing

Although Bayesian network structure can be created by experts based on domain knowledge [11], more researches are interested in learning Bayesian network from data automatically. Learning structure is more crucial part of the whole course and the final results are directly related to it. Recently many methods for structure learning have been developed, finding the structure that is most suitable to training data. The score based search method uses approximate search algorithms to construct candidates and measures them using scoring evaluation. The dependency analysis method starts with analyzing dependency relationships between nodes to construct a network. However, both methods are not suitable when there are larger data, which in this case brings overfitting which is one of the main issues in using machine learning. The overfitting phenomenon occurs when too many parameters are considered in a given domain. In building Bayesian network structure, it occurs when considering too many parameters in structure learning. So in order to solve such problems and make structure learning more efficient, we can provide preconditioning course previously.

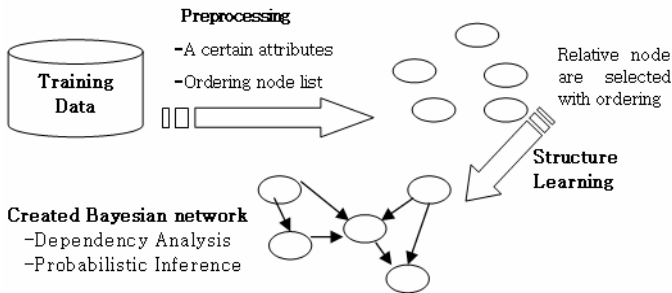


Fig. 2. Preprocessing of Training data

Fig.2 depicts the process before Bayesian network structure learning. Given training data, it selects certain relative factors with ordering, and then enters into the step of structure learning, on which probabilistic dependency analysis are based.

There are two phases included in preprocessing. First, from the given large dataset with more parameters, it can only consider factors that are more relative with focusing problems, i.e. choose relative factors describing the domain. We can downsize the number of factors by using information theory method to analyze relationships or clustering or other approaches. After determining certain factors, it arranges them in a special order, which means anterior one has direct influence on the posterior one in the same direction of arrow, by analyzing information gain between pairs of observing data. However, it emphasizes the assumption is that problematic parameters

are independent of each other when learning structure. All parameters in the ordering lists are able to have influence on each problematic parameter; thereby each problematic problem has the same ordering list only with each different problematic factor as the last one, which implies that all the factors in front of it could be a parent node of the last one. The pseudo code of the ordering algorithm is described as follows.

Input: Separate observing parameters from problematic parameters stored in set $S = \{V_1 \dots V_n, P_1 \dots P_m\}$.

Output: An ordering list with a certain number of parameters

1) Select a certain observing parameters with high relevance to problematic parameters.

for each problematic parameter P_j ($j = 1$ to m) do

for $i = 1$ to n do

compute information gain $G_{ij} = \text{Gain}(V_i, P_j) = H(P_j) - H(V_i, P_j)$ ($H()$ means entropy)

end for

rank parameters with G_{ij} from maximum to minimum and save them to list L_j

end for

Combine all lists L_j ($j = 1$ to m), select observing parameters with the mean information gain exceeds defined threshold value.

Return the selected parameters and all problematic parameters. $S' = \{V_1 \dots V_k, P_1 \dots P_m\}$ ($k < n$)

2) Make an ordering list for the selected observing parameters in set S'

Initialize set $S'' = \{V_1, \dots, V_k\}$ except for problematic parameters; pair set $P = \{\text{empty}\}$; list $L = \{\text{empty}\}$

Select two parameters V_x and V_y from the head of set S'' ($x \neq y$)

Compute $\text{Gain}(V_x, V_y)$ and $\text{Gain}(V_y, V_x)$ for each pair, put pair $(V_x \rightarrow V_y)$ with larger Gain into set P stop when there is close loop, run until all parameters in set S'' are considered.

Sort the pairs in set S'' to a single ordering list L

Return an ordering list L only with observing parameters

Applying an ordering node list into the next step of learning, for score based search method, it can reduce the entire search space when adding link to construct network, as a node can be parent only of node which is behind it according to the ordering node list; for dependency analysis method, it can reduce computing complexity as the number of nodes is decreased and determine the direction between two nodes.

3.4 Structure Learning

In this paper, an ordering node list with certain parameters is used as input to create a fine-grained model by analyzing conditional independency evaluation, which determines dependency relationships between all pairs of nodes. It should be stressed at this point that Bayesian network implies conditional independencies via showing conditional probability tables for leaf nodes having direct parent nodes.

Bayesian network structure learning from data presents an efficient algorithm based on the conditional independence (CI) test to measure dependency relationships [12]. In this paper, one of the structure learning mechanisms, which begin with the definition of Bayesian network, is based on computing mutual information introduced in the Information Theory for pairs of nodes to reflect different degrees of dependency relationships among them. A threshold is given to determine the existence of probabilistic dependency relationship between nodes.

4 Experiment and Evaluation

Following the rapid growing internet systems in the Ubiquitous computing era, violations of service level objectives [13] are related to reliability of system and quality of service. As automated management capability described in self-managing, when there are faults such as bottlenecks, violation of Service Level Objectives occurred, the system should find which factor is directly related to them and affect high level performance of system automatically, by analyzing observed parameters consisting of performances of individual servers or processes, capability of network, hardware and software, dynamic variation resource utilizations by different types of client requests, and temporary traffic situation. Thereby, they can be used to determine which part of the system is responsible for current fault of the system, then it is repaired appropriately; oppositely, the collected information can be used to forecast system potential problems, preventing them in advance.

In our experiment, it collects and filters data of interest that can be used for analysis, including CPU, memory, disk utilization, count of client, package volume, bandwidth logged in a server and detects information such as threshold violation in response time and throughput, on which we rely to analyze and control system management for providing high quality of service and performance, as described in Table 1. Then, after collecting sample data, each parameter should be categorized into corresponding classes according to given criteria, such as High, Medium, Low for performance parameters and Error, warning, normal for problematic parameters.

Table 1. Training parameters

| System metrics (Performance parameters) | | | | | | Bottlenecks, SLO violation | | |
|---|----------|-----------|----------|--------------|-----------|----------------------------|---------------|------------|
| CPU uti. | RAM uti. | Bandwidth | Filesize | Client count | Disk uti. | ... | Response time | Throughput |
| 70% | 67% | 3.1 | 35 | 159 | 72% | ... | 3.6 | 65 |
| 65% | 58% | 2.8 | 28 | 132 | 58% | ... | 4.1 | 58 |
| 56% | 72% | 4.6 | 42 | 126 | 69% | ... | 3.6 | 43 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 49% | 61% | 3.1 | 38 | 110 | 50% | ... | 4.5 | 57 |

$$S = \{V_{cpu}, V_{ram}, V_{disk}, V_{bandwidth}, V_{client}, V_{filesize}; P_{response}, P_{throughput}\}$$

We take above parameters as input to create node ordering with certain number of parameters which are highly related to problematic parameters. After learning on the training data, the result of selecting relative parameters is:

$$S' = \{V_{bandwidth}, V_{client}, V_{ram}, V_{cpu}; P_{response}, P_{throughput}\}$$

Then the observing parameters are ranked by using the proposed approach to output a node ordering list without problematic parameters, as follows:

$$Orderinglist = \{V_{cpu} \rightarrow V_{ram} \rightarrow V_{bandwidth} \rightarrow V_{client} \rightarrow P_{response}, P_{throughput}\}$$

With the predefined assumption, the problematic parameters response time and throughput are independent of each other. From the above ordering list, it implies that the node orderings can be used when constructing a Bayesian network.

$$P = \{V_{cpu} \rightarrow V_{ram}, V_{ram} \rightarrow V_{bandwidth}, V_{bandwidth} \rightarrow V_{client}, V_{client} \rightarrow V_{response}, V_{client} \rightarrow V_{throughput}\}$$

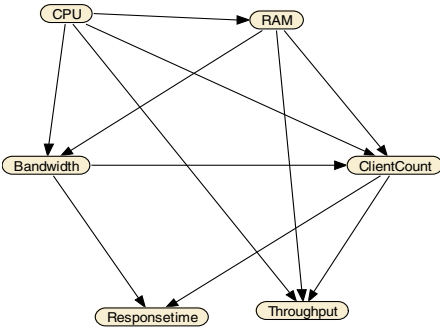


Fig. 3. Structure Learning

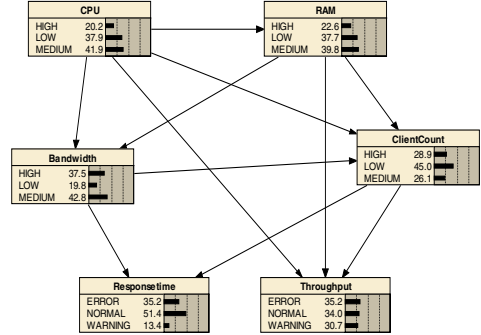


Fig. 4. Parameter Learning

From Fig. 3 we can see that the created structure is a compact hierarchy model after learning from certain parameters and ordering list. In contrast to the simple structure of Naïve Bayesian network, it discovers and represents internal dependency relationships between each pair of causal parameters in the network structure, which makes the results of inferences more accurate. The next learning phase is parameter learning given structure and training data i.e. fixing conditional probabilities for each node. Fig.4 describes the complete Bayesian network after parameter learning.

The inference courses based on probabilistic dependency analysis can be carried out given the created model, and including inductive and deductive reasoning. Given the convinced states of several parameters, it makes the known state with 100% belief, which operation can change beliefs of all nodes that related to such one after probability being propagated throughout the whole network. For instance, a violation of response time is occurred that makes response time be of error state, the most probable impact factor can be found that low class of bandwidth with the highest probability; on the other hand, when the utilization of CPU resource arrives at 95% utilization which belongs to high class with 100% evidence, the probability of error state of throughput can get up to be the highest, which means that there will be a fault of throughput appeared in coming time. These results derived from diagnosis and prognosis are very helpful for system to take correct repairs to figure out faults or to avoid potential faults in advance. From the probabilistic network, it's easy for us to understand how the factors affect each other by changing the evidences of nodes with dynamic representation.

However, in order to estimate the effect of inference following our approach, we apply testing data into the built model then compare the results with the actual outcome. At first, we evaluate the time consumption of structure learning and error rate given different numbers of parameters, showing the obvious effect of using a certain number of parameters that highly correlate with the domain. From Fig. 5, we can find that as the number of parameters grows, the time consumption mounts up but the error rate of detecting faults drops and the number of parameters corresponding to the crossing of two curves can be chosen as an appropriate quantity for considering the parameters in such a domain.

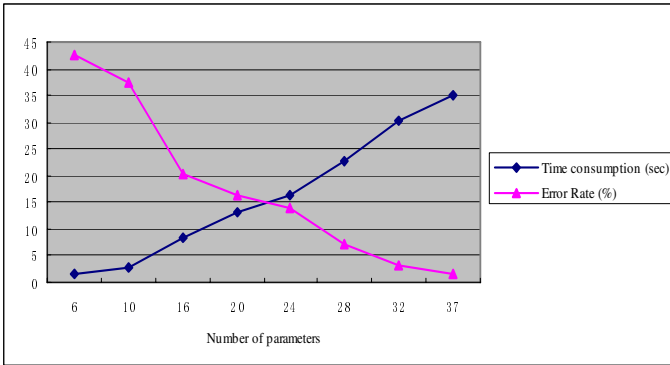


Fig. 5. Evaluation with different number of nodes

Furthermore, comparison of time consumption and accuracy is evaluated in the case of selecting 24 parameters regardless of being provided with a node ordering list. Table 2 can tell us that with the node ordering list, there are improvements both in time consumption and accuracy of inferring results.

Table 2. Comparison on cases with and without node ordering

| Dimensions | Time consumption (sec) | Accuracy (%) |
|-----------------------|------------------------|--------------|
| with node ordering | 15.48 | 90.3 |
| without node ordering | 16.37 | 85.2 |

In conclusion, the comparison of structure learning under a given certain quantity of parameters and ordering list, points out taking the ordering list as input of structure learning accounts for that preconditioning of parameters in the process is much more effective, regardless of whatever learning method is used.

5 Conclusion

In this paper, a Bayesian Network based mechanism of problem localization for automated system management in Ubiquitous computing is proposed. In order to improve the performance of learning with domain knowledge, a preprocessing step which reduces the size of parameters is added to improve the whole process of Bayesian network modeling. Using the proposed methods, we can transform a complex system into a compact model with high efficiency and accuracy, on which we depend to make inference via probabilistic dependency analysis. In contrast to other existing researches on using Bayesian network, it can process input data in advance, which is implemented with high accuracy to improve the efficiency of structure learning. In order to prove availability of the proposed approach, we perform it in the system performance domain to achieve automated system management and make various comparisons under different conditions.

Our future work will continue to research on machine learning, which is considered as an Artificial Intelligent approach for self-managing system to learn real-life streams of events that expresses health states and faults. There are many algorithms[14] used in various fields for machine learning, including time-series, decision Tree, case-based reasoning, rule based reasoning and so on. Following these methods, it can provide multiple functions in fields of diagnosis, prognosis, fault isolation and root cause analysis.

References

1. Sahoo, R.K., Oliner, A.J., Rish, I., Gupta, M., Moreira, J.E., Ma, S., Vilalta, R., Sivasubramaniam, A.: Critical event prediction for proactive management in large-scale computer clusters. In: Proceedings of the ACM SIGKDD, Intl. Conf. on Knowledge Discovery and Data Mining, August, pp. 426–435 (2003)
2. Kephart, J.O., Chess, D.M.: IBM Thomas J. Watson Research Center: The Vision of Autonomic Computing. IEEE Computer Society, Los Alamitos (2003)
3. Steinder, M., Sethi, A.S.: A Survey of Fault Localization Techniques in Computer Networks. Science of Computer Programming. Special Edition on Topics in System Administration 53(2), 165–194 (2004)
4. Yoo, G., Park, J., Lee, E.: Hybrid Prediction Model for improving Reliability in Self-Healing System. In: SERA 2006. ACIS International Conference on Software Engineering Research, Management & Application, pp. 108–115. IEEE Computer Society, Los Alamitos (2006)
5. Rish, I., Brodie, M., Ma, S., Odintsova, N., Beygelzimer, A., Grabarnik, G., Hernandez, K.: Adaptive Diagnosis in Distributed Systems. IEEE Transactions on Neural Networks (March 2005)
6. Dai, Y.-S.: Autonomic Computing and Reliability Improvement. In: ISORC 2005. Proceedings of Eighth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, pp. 204–206 (2005)
7. IBM Self-Aware Distributed Systems:
<http://domino.watson.ibm.com/comm/research.nsf/pages/r.ai.innovation.2.html>
8. Sun Microsystems: Predictive Self-Healing in the Solaris 10 Operating System:
<http://www.sun.com/bigadmin/content/selfheal>
9. Alpaydm, E.: Introduction of Machine Learning. © 2004, Massachusetts Institute of Technology
10. Charles River Analytics Inc: About Bayesian Belief Networks. © Copyright, Charles River Analytics, Inc. (2004)
11. Ding, J., Kramer, B., Bai, Y., Chen, h.: Backward Inference in Bayesian Networks for Distributed Systems Management. Journal of Network and Systems Management 13(4) (2005)
12. Cheng, J., Bell, D.A., Liu, W.: An Algorithm for Bayesian Belief Network Construction from Data. In: Proceedings of AI & STAT, pp. 83–90 (1997)
13. <http://www.risi.com/services/sla.html>
14. Vilalta, R., Apte, C.V., Hellerstein, J.L., Ma, S., Weiss, S.M.: Predictive algorithms in the management of computer systems. IBM Systems Journal issue 41-3, Artificial Intelligence 41(3) (2002)

A High Speed Analog to Digital Converter for Ultra Wide Band Applications

Anand Mohan, Aladin Zayegh, and Alex Stojcevski

Centre for Telecommunications and Microelectronics
School of Electrical Engineering
Victoria University
P.O. Box 14428
Victoria 8001, Australia
anand.mohan@research.vu.edu.au

Abstract. Over the past few years Ultra Wide Band (UWB) technology has taken the realms of communications circuit design to new levels. This paper demonstrates the design and simulation of a very high speed Flash Analog to Digital Converter (ADC) for UWB applications. The ADC was implemented in 90 nanometre (nm) CMOS design process. The converter works at an optimal sampling rate of 4.1 Gig-Samples per second (Gsp/s) for an 800 MHz input bandwidth corresponding to a 1V full scale reference. The converter has moderate linearity error tolerance of about ± 1 LSB (62.5 mV) without use of any averaging techniques. The ADC works on a 1V supply and has an overall power consumption of 114 mW.

Keywords: ADC, UWB, CMOS Technology, Flash Topology, Power Saving.

1 Introduction

The deregulation of the UWB frequency spectrum by the Federal Communications Commission (FCC) and subsequently by other countries has offered a tremendous boost to communications and applications that require a medium to transfer large amounts of data in a very short period of time. UWB offers an unparalleled medium for such high speed communications, with an effective transmitting bandwidth of almost 7.5 GHz. This means that data transmission in the range of few tens to hundreds of gigabits per second are now realisable. UWB transmission consists of signals that are in the form of sub-nanosecond pulses and are therefore transmitted and received at short distances but over a very large frequency range. Applications for UWB range from commercial high speed wireless access to very high data rate medical imaging systems. Typical UWB systems are characterized as having a signal bandwidth of 528 MHz or more. UWB offers advantages in its ability to resist multipath fading and jamming from nearby nodes, low spectral density and a very high channel capacity [1], [2].

The application of Shannon's Channel Capacity equation highlights the unique ability that UWB offers. The equation defines a unique relationship between the maximum data rate and the total transmission bandwidth, as seen in Equation 1.

$$C_x = f_x * \log \left[\frac{P_r}{N_t * f_x} \right] \quad (1)$$

where C_x corresponds to the channel capacity, f_x is the channel bandwidth, N_t is the power spectral density of noise and P_r if the received power into the system [3].

The ADC being the heart of the system provides a unique challenge in its design for such high speed requirement. Section 2 details out UWB receiver and its characteristics. Section 3 details out the high speed ADC architecture, while section 4 gives an overview of obtained results.

2 UWB Receiver

Typically ideal UWB systems consist of a receiver chain with minimal components as illustrated in Fig. 1. The receiver front-end consists of a very large bandwidth Low Noise Amplifier (LNA), Variable Automatic Gain Control Amplifier (VGA) and Very High Speed ADC. The advantage that this architecture offers is a reduction in the total number of components in the front-end and an overall saving in power.

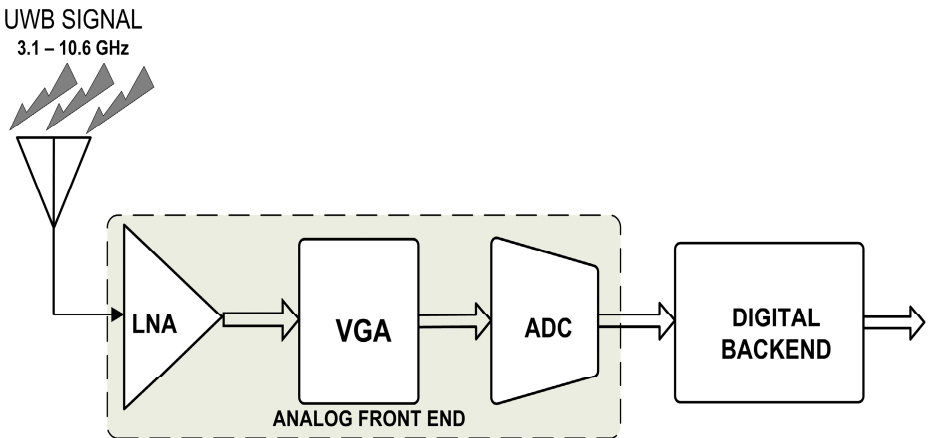


Fig. 1. Ideal UWB Receiver

For such a setup to be implementable would require a LNA to handle frequencies from 3.1 GHz to 10 GHz, VGA to provide amplification and stabilisation from about -25 dBm to 0 dBm and an ADC to operate full scale at a minimum sampling frequency of 7 Gsps. This type of specification range will require CMOS systems to

switch and thereby adjust to changing frequency ranges in a matter of few of picoseconds. For an ADC to effectively sample (Nyquist Rate) a 4 GHz input signal will require to have a clock with switching speed of 125 picoseconds. The fastest Flash converters [4] require all comparators to switch and work in perfect synchronisation. For low resolution converters the numbers of comparators are minimal, however in presence of mismatch and linearity problems, will require converters to have larger resolutions. Moreover with flash converters a single bit increase in resolution leads to a doubling in power consumption and thereby requiring preamplifier input bandwidth of more than 200 GHz. Present CMOS technology cannot switch efficiently at such high speeds without encountering mismatch and large scale linearity problems [4].

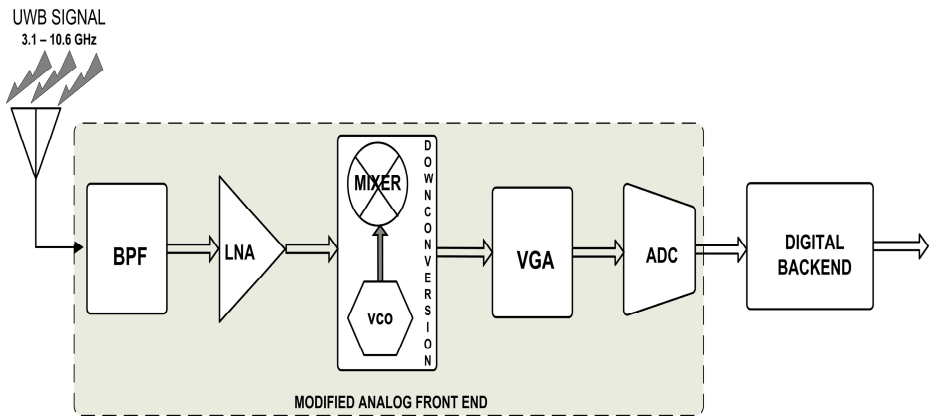


Fig. 2. Down-converted UWB Receiver

A more realistic approach is illustrated in Fig.2. A down conversion stage comprising of a mixer and a Voltage Controlled Oscillator (VCO) is used to reduce the frequency range to hundreds of megahertz to a few gigahertz. This intermediary setup relaxes the requirements on the ADC such that a very high speed digitiser can be realised in CMOS effectively [4], [5].

3 ADC Architecture

This section details out the design of the ADC for use in UWB systems. From [6] it can be estimated that for a Gaussian 5th order down-converted frequency spectrum, having a effective bandwidth of 600MHz or more and residing in a frequency range of 1.3 GHz to 2.5 GHz, an over-sampled converter working at 4 Gsps is more than sufficient. Based on calculations in [5-7] it is seen that 4 bits are the optimum resolution to ensure reliable detection. A number of ADC architectures were looked into and analysed comprehensively [8]. It is seen that among all architectures Flash

based architecture is the most suitable choice for implementation. The parallel nature of Flash ADC with its array of synchronised comparators provides the fastest solution for UWB implementation [9-11].

The entire structure of the designed ADC is shown in Fig.3. It consists of a differential resistor ladder that provides full scale reference for all the comparators. A flash architecture consists of $2^X - 1$ comparators for X bits, hence the ADC in this work consists of 15 comparators. Section 3.1 details the design of the high speed fully differential comparator and section 3.2 details out the design of a high speed MOS Common Mode Logic (MCML) Encoder.

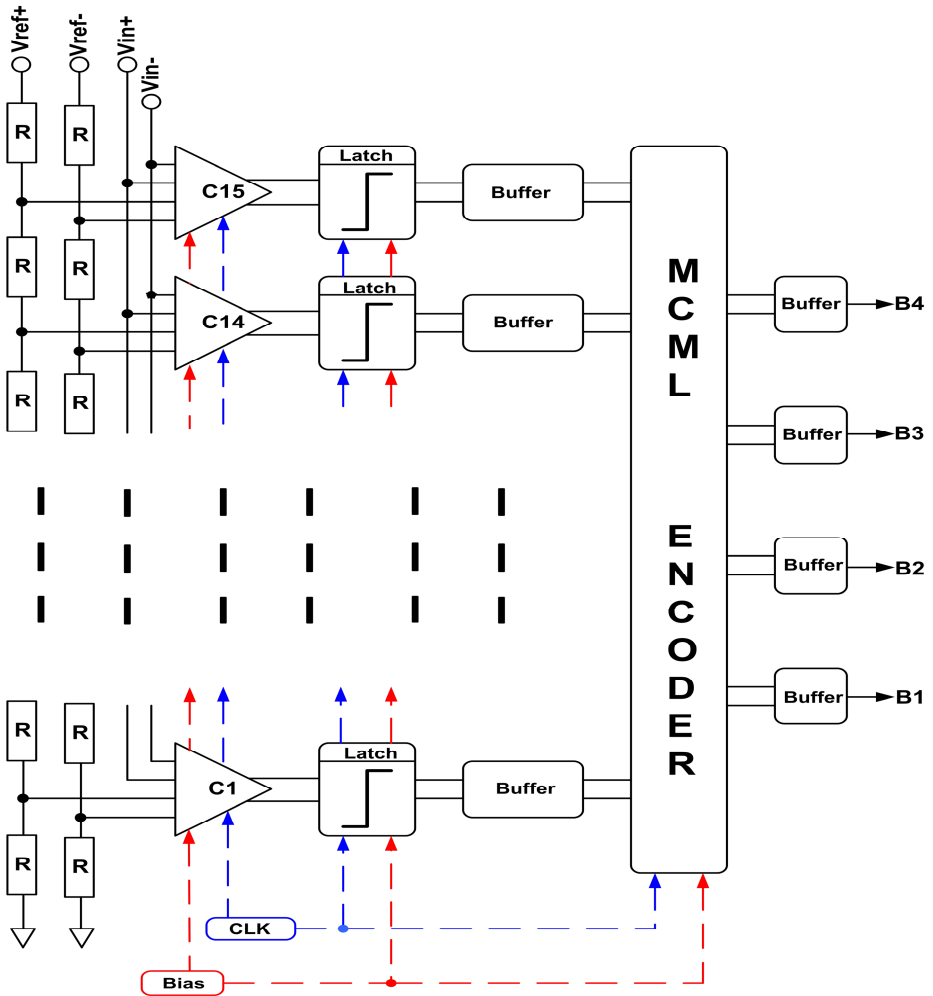


Fig. 3. ADC Architecture

3.1 Comparator Design

The comparator depicted in Fig. 4. is a low voltage fully differential three stage design. The first stage consists of an input pre-amplifier and two consecutive latches. The first latch is a differential track and hold latch while the second is a high speed regenerative latch.

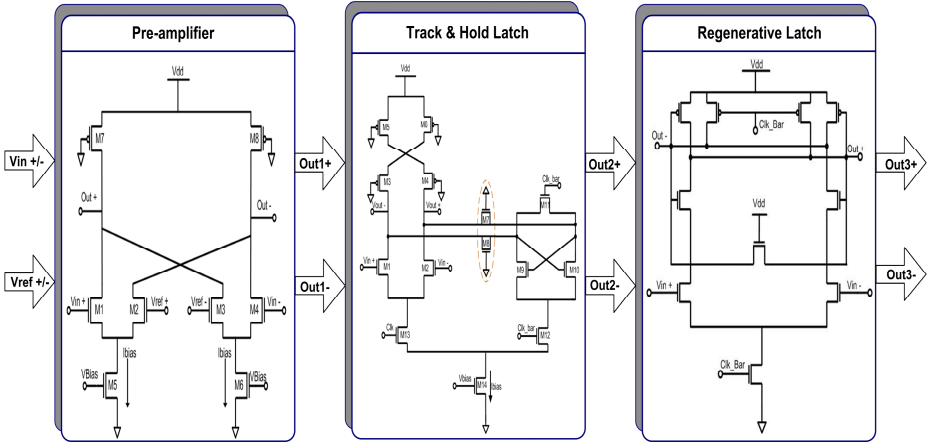


Fig. 4. Comparator

Input Pre-amplifier. The pre-amplifier as shown in Fig. 4. is a fully differential open loop architecture. This architecture provides many advantages over closed loop structures due to its high speed, low swing and low gain. The open loop structure also offers reduced power consumption and better rejection of V_{DD} noise. The pre-amplifier has an intrinsic gain defined by (g_m/g_{ds}) , keeping in mind its low gain nature. Close to minimum length transistors are used for all the input differential pairs to ensure that there are reduced offset problems and ensure faster switching. The pre-amplifier is loaded with triode loads. This type of loading helps to keep the output slew rate to a minimum and also offers required voltage headroom. The input referred offset of the pre-amplifier was estimated based on Equation 2.

$$V_{os} = \left[\frac{\Delta L_{N-i}}{L_{N-i}} + \dots + \frac{\Delta L_i}{L_i} + \frac{\Delta W_{N-i}}{W_{N-i}} + \dots + \frac{\Delta W_i}{W_i} \right] + V_T \tag{2}$$

where V_{os} is the offset voltage, L_{N-i} is the length of the transistors change and W_{N-i} is the width of the transistor change for the input pairs [12], [13].

Track and Hold Latch. The latch is shown in Fig.4. It provides very low swing and very high speed operation. The latch is based on a clocking scheme such that whenever the clock is high the input pairs are active and track in the input from the

pre-amplifier. When the clock goes low the latch provides slight positive feedback and amplification. Like the pre-amplifier the latch also uses a cascaded cross coupled triode load that helps in the low swing operation. This loading scheme has advantage in that it helps to reduce the V_{DD} noise variation on the input pairs. The output settling time was optimised by setting the common mode voltage (V_{CM}) of the latch, as shown in Equation 3 [12], [13]. This type of latch has good slew rate and also provides sufficient tolerance to meta-stability problems [14].

$$V_{CM} = \frac{V_{DD}}{2} \quad (3)$$

Regenerative Latch. The final stage of the comparator is a regenerative latch (Fig. 4.) based on [13], [14]. The latch is used primarily to pull the output to logic rail to rail levels. The working of the latch is based on a clock that switches on the input pairs when the clock is high. When the clock is low it provides feedback and pre-charges the output to V_{DD} . The latch is self-biased and therefore offers a great saving in power consumption. The latch is sized to provide the required output swing. The output capacitances provide slightly different discharging times to enable proper feedback [13], [14].

3.2 Encoder

Fig. 5. shows the schematic of a high speed encoder. The encoder was based on a thermometer to binary conversion with an intermediate gray code stage. The gray code stage provides only a 1 bit transition between consecutive states and thereby reduces the effects of code skipping and bubble errors at the output of the encoder. The encoder is designed used MOS Common Mode Logic (MCML). This type of design is the most efficient in terms of speed and very low swing signal operation. The encoder was designed such that the 15 outputs from the comparators are fed through a series of NAND/AND gates such that they are converted to 4 bit gray code and then re-converted from 4 bit gray code to a 4 bit binary output [15].

The design equations for the implementation of the encoder are highlighted below. A set of equations (Equation 4.) shows the conversion from thermometer to gray code and another set of equations (Equation 5.) shows the succeeding conversion from gray to 4 bit binary.

Thermometer to Gray Code Conversion:

$$\begin{aligned} K1 &= \overline{C1C3} \cdot \overline{C5C7} \cdot \overline{C9C11} \cdot \overline{C13C15} \\ K2 &= \overline{C2C6} \cdot \overline{C10C14} \\ K3 &= C4\overline{C12} \\ K4 &= C8 \end{aligned} \quad (4)$$

Gray to Binary Code Conversion:

$$\begin{aligned}
 B_1 &= K_1 \oplus B_2 \\
 B_2 &= K_2 \oplus B_3 \\
 B_3 &= K_3 \oplus B_4 \\
 B_4 &= K_4
 \end{aligned}
 \tag{5}$$

The output of the encoder is then buffered to get a sharp switching response with minimal rise and fall times.

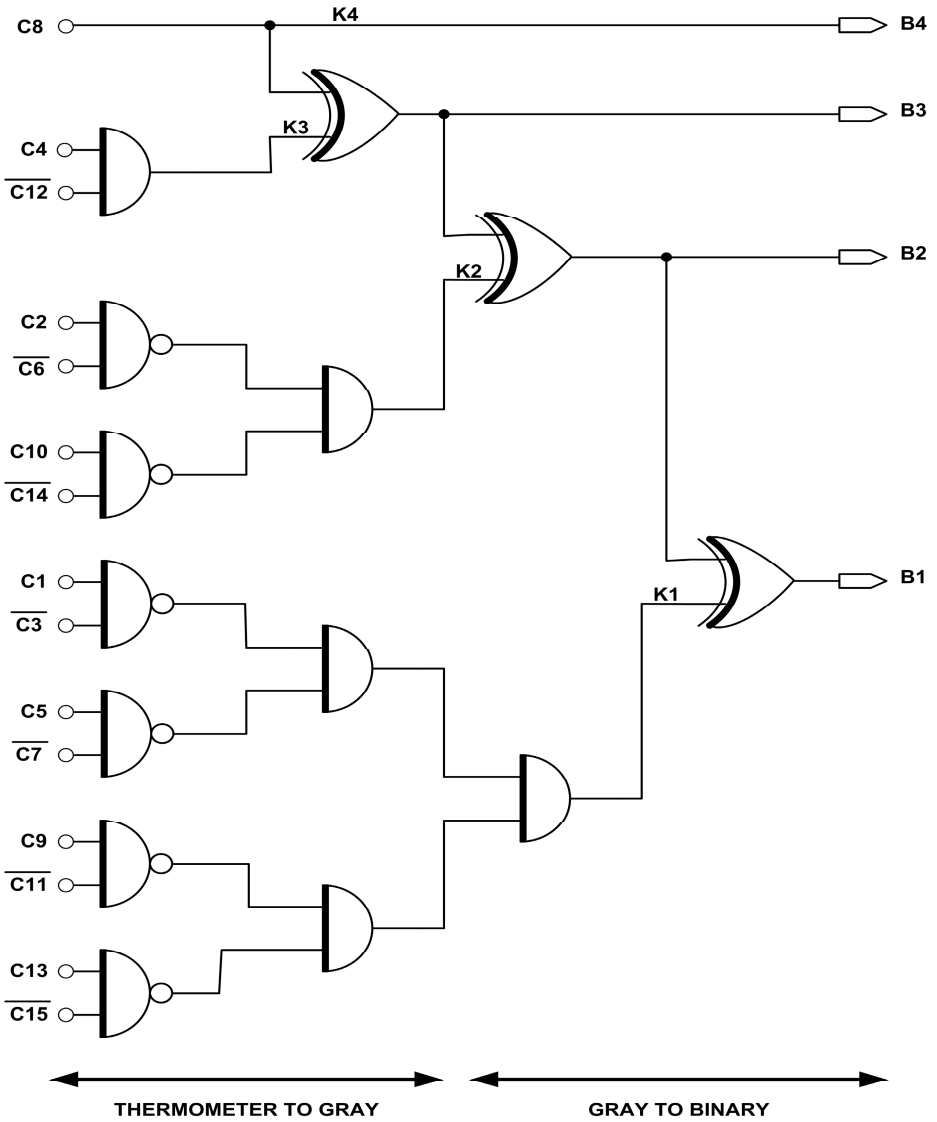


Fig. 5. Encoder

Fig. 7. to Fig. 9. show the linearity error variance and Spurious Free Dynamic Range (SFDR) for the 4 bit ADC. Fig. 10. Shows the different trip points for each of the comparators.

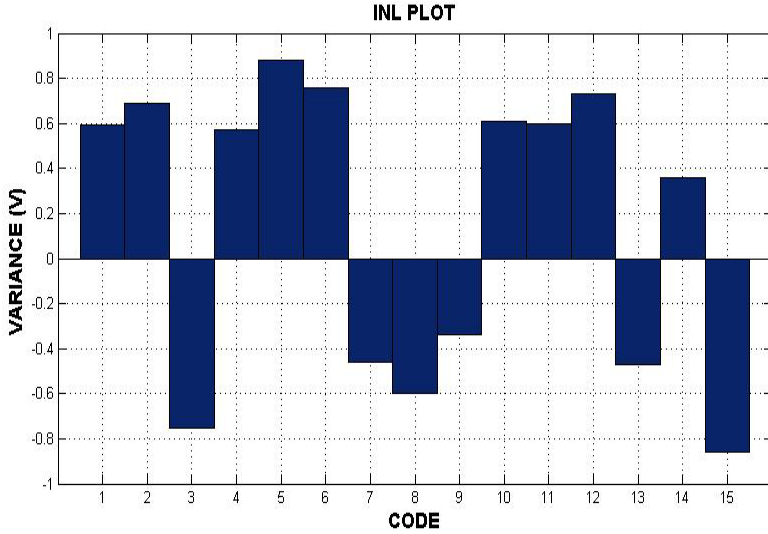


Fig. 7. Integral Non-Linearity Plot ($f_{IN} = 800$ MHz @ $f_S = 4.1$ Gps)

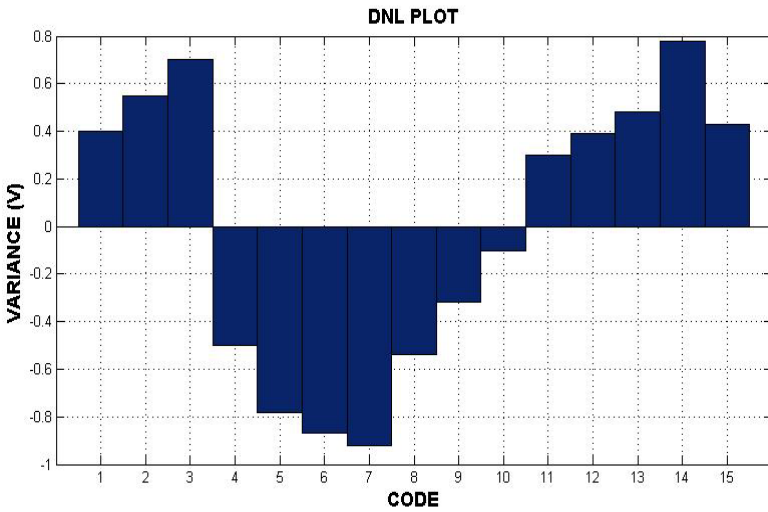


Fig. 8. Differential Non-Linearity Plot ($f_{IN} = 800$ MHz @ $f_S = 4.1$ Gps)

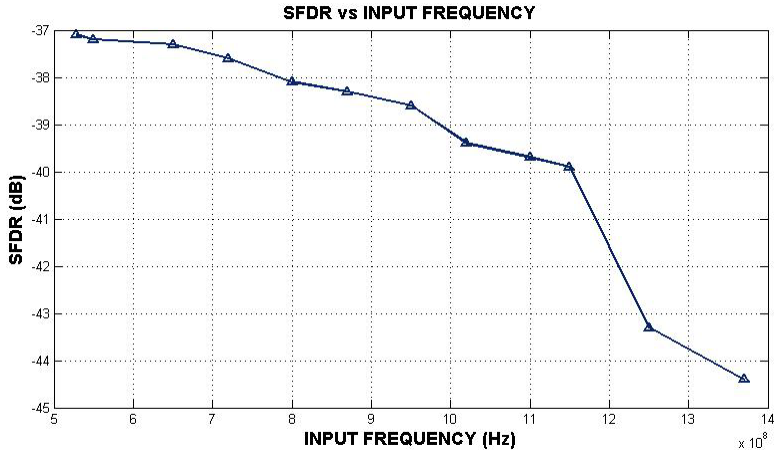


Fig. 9. Plot of SFDR versus Input Frequency

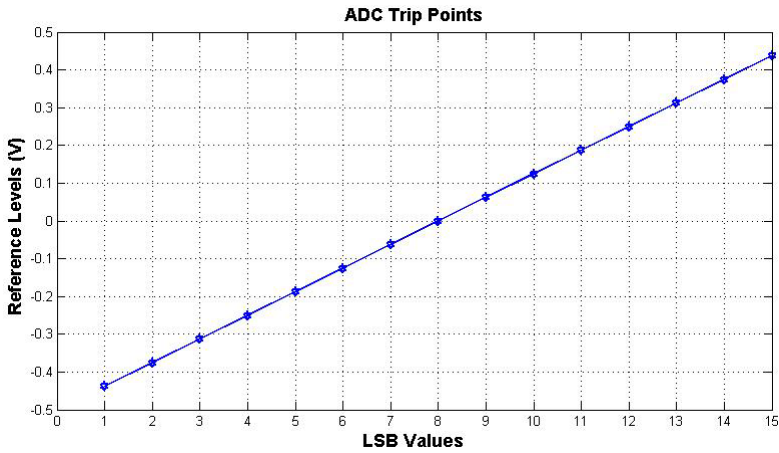


Fig. 10. Plot of ADC Trip Points

The performance characteristics of the ADC are detailed in Table 1. The entire ADC consumes 114 mW of power at input of 800 MHz sampled at 4.1 Gps. The ADC has a linearity error variance of not more than ± 1 LSB. No Averaging or Interpolation techniques have been used to minimise the effects of offset. The encoder has been sized such that it has a maximum critical path delay of 0.234 ns. The encoder does not have any dynamic pipelining stages as there is no monotonicity error in the ADC, thereby reducing overall power dissipation.

Table 1. ADC Performance Characteristics

| Parameter | Performance Characteristic | | [19] | [20] |
|------------------------------|---|--------------------------------------|------------------------|-----------|
| Input Signal Range | Sinusoidal 1 V p-p differential | Sinusoidal 1 V p-p differential | 0.8 V p-p | 1.6 V p-p |
| Input Frequency | 800 MHz | 1120 MHz | - | 650 MHz |
| Resolution | 4 bits (1LSB = 62.5 mV) differential | 4 bits (1LSB = 62.5 mV) differential | 4 bits | 6 bits |
| Supply Voltage | 1 V | 1 V | 1.8 V | 3.3 V |
| Sampling Rate | 4.1 Gsps | 4.1 Gsps | 3.2 Gsps | 1.3 Gsps |
| Maximum Sampling Rate | 6.3 Gsps | 6.3 Gsps | 3.2 Gsps | 1.3 Gsps |
| Maximum INL | -0.82 V / +0.84 V | -0.96 V / +1.1 V | 0.6 LSB | 0.35 LSB |
| Maximum DNL | -0.92 V / +0.76 V | -1.4 V / +1.1 V | 0.4 LSB | 0.2 LSB |
| SFDR | -38.2 dB | -41.3 dB | - | > 44 dB |
| ENOB (@ 800 MHz) | 3.45 | 3.1 | 3.6 | > 5.5 |
| Power | 114 mW (@ 4.1 Gsps) | 176 mW (@ 4.1 Gsps) | 131 mW | 500 mW |
| Structure | Non-Time Interleaved | | 2 Way Time Interleaved | Averaging |
| Technology | ST-Microelectronics 90 nm Standard V _T CMOS | | 0.18 um | 0.35 um |

5 Conclusion

This paper presents the design and of a high speed Flash Analog to Digital Converter for Ultra Wide Band Applications. The ADC achieves moderate linearity and resolution without the use of any power hungry offset averaging techniques. The Effective Number of Bits (ENOB) for a 800 MHz input is estimated as 3.45. The encoder was sized to provide high speed conversion with no pipelining. The ADC has very low gain low swing. No digital backend processing was required to correct ADC errors, such as mismatch and monotonicity.

Acknowledgments. The authors would like to thank Mr. David Fitrio for his technical expertise and critical insights.

References

1. Federal Communications Commission: First Report and Order: Revision of Part 15 of the commissions rules regarding ultra wideband systems, ET Docket No. 98-153, FCC (2002)
2. Australian Communications and Media Authority: Use of ultra wideband approved for the first time, Media Release, Media Release No. 24 (April 2004)
3. Oppermann, I., Hamalainen, M., Iinatti, J.: UWB: Theory and Applications. WILEY International Publishers, Chichester (2004)
4. Newaskar, P., Blazquez, R., Chandrakasan, A.: A/D precision requirements for digital ultra-wideband radio receivers. *J. of VLSI Signal Processing Systems for Signal, Image, and Video Technology* 39, 175–188 (2005)
5. Romdhane, M., Loumeau, P.: Analog to digital conversion specifications for ultra wide band reception. In: Proc. of the Fourth IEEE Intl. Sym. on Signal Processing and Information Technology, December, pp. 157–160 (2004)
6. Fischer, R., Kohno, R.: DS-UWB Physical Layer Proposal Submission to IEEE 802.15 Task Group 3a (September 2005)
7. Roberts, R.: XtremeSpectrum CFP Document, IEEE P802.15-03/153r8 (July 2003)
8. Geelen, G.: A 6 b 1.1 GSample/s CMOS A/D converter, ISSCC Dig. Tech. Papers, pp. 128–129 (2001)
9. Walden, H.R.: Analog to Digital Converter Survey and Analysis. *IEEE J. on Selected Areas in Comm.* 17, 539–550 (1999)
10. Yoo, J., Choi, K., Tangel, A.: A 1-GSPS CMOS Flash A/D Converter for System-on-Chip Applications. In: IEEE Computer Society Workshop on VLSI, pp. 135–139 (2001)
11. Stojcevski, A., Le, H.P., Singh, J., Zayegh, A.: Flash ADC Architecture. *IEEE Electronic Letters* 39, 501–502 (2003)
12. Mohan, A., Zayegh, A., Stojcevski, A., Veljanovski, R.: Comparator For High Speed Ultra Wideband A/D Converter. In: Proc. of the Intl. Conf. on Communication, Computer and Power (February 2007)
13. Mohan, A., Zayegh, A., Stojcevski, A., Veljanovski, R.: High Speed Ultra Wide Band Comparator in Deep Sub-Micron CMOS. In: ISIC 2007. Intl. Sym. On Integrated Circuits (in print)
14. Heo, S., Krashinsky, R., Asanovi'c, K.: Activity-Sensitive Flip-Flop and Latch Selection for Reduced Energy. In: 19th Conference on Advanced Research in VLSI (March 2001)
15. Razavi, B.: Principles of Data Conversion System Design. IEEE Press, Los Alamitos (1995)
16. Ismail, A., Elmasry, M.: A low power design approach for mos current mode logic. In: Proc. of 2003 IEEE Intl. SOC Conference, September, pp. 143–146 (2003)
17. Khabiri, S., Shams, M.: Implementation of mcml universal logic gate for 10 ghz-range in 0.13 μm cmos technology. In: Proc. of IEEE Intl. Symp. on Circuits and Systems, vol. 2, pp. 653–656 (2004)
18. Anis, M., Elmasry, M.: Self-timed mos current mode logic for digital applications. In: Proc. of IEEE Intl. Symp. on Circuits and Systems, vol. 5, pp. 113–116 (May 2002)
19. Naraghi, S., Johns, D.: A 4-bit analog-to-digital converter for high-speed serial links. In: Micronet Annual Workshop, Aylmer, Quebec, Canada, April 26–27, pp. 33–34 (2004)
20. Choi, M., Abidi, A.: 6-b 1.3-Gsample/s A/D Converter in 0.35 μm CMOS. *IEEE Jnl. of Solid State Circuits* 36(12), 1847–1858 (2001)

Design and DSP Software Implementation of Mobile WiMAX Baseband Transceiver Functions

Hai-wei Wang¹, David W. Lin¹, Kun-Chien Hung¹, and Youn-Tai Lee²

¹ Dept. Electronics Engineering and Center for Telecommunications Research
National Chiao Tung University, Hsinchu, Taiwan, R.O.C.

² WiMAX Technology Center, Network and Multimedia Institute
Institute for Information Industry, Taipei, Taiwan, R.O.C.
c93jo6@gmail.com, dwlin@mail.nctu.edu.tw,
hkc.ee90g@nctu.edu.tw, lyt@nmi.iii.org.tw

Abstract. This paper considers the orthogonal frequency-division multiple access (OFDMA) physical layer of the IEEE 802.16e standard. We discuss the design of some key baseband signal processing functions, including synchronization, channel estimation, and forward-error-correction (FEC) decoding. Further, we describe a fully software implementation of these functions employing Texas Instruments' digital signal processors (DSPs).

Keywords: Channel estimation, digital signal processor (DSP) software implementation, bit-interleaved coded modulation, IEEE 802.16e, orthogonal frequency-division multiple access (OFDMA), synchronization, WiMAX.

1 Introduction

An increasing amount of programmability is being required of wireless communication devices. For handheld mobile devices, a completely software implementation is still not viable for cost and power consumption reasons, but to some degree one may not be able to fully ignore such a possibility in view of the proliferating wireless communication standards and the envisioned emergence of cognitive radio. For infrastructure devices such as base stations (BSs), on the other hand, the economical balance appears to tip comparatively more towards implementing many of the required signal processing functions in software. In either case, a fully software implementation is at least a useful tool that can serve various prototyping and functional verification purposes.

In this study, we consider the IEEE 802.16e orthogonal frequency-division multiple access (OFDMA) physical layer (PHY), which has been adopted in Mobile WiMAX. We discuss the design of some key baseband signal processing functions and describe a fully software implementation of these functions employing Texas Instruments' digital signal processors (DSPs).

The paper is organized as follows. Section 2 provides an overview of the relevant IEEE 802.16e OFDMA PHY specifications. Section 3 discusses three key

signal processing functions to some depth, namely, synchronization, channel estimation, and forward-error-correction (FEC) decoding. Section 4 presents some simulation results on their performance. Section 5 describes the DSP software implementation. Finally, Section 6 is the conclusion.

2 Overview of the IEEE 802.16e OFDMA PHY

Orthogonal frequency-division multiplexing (OFDM), by its use of cyclic prefixing (CP), is known to be able to combat multipath interference easily. The OFDMA PHY in IEEE 802.16e further divides the subcarriers into subchannels that can be allocated individually. This provides flexible access control in frequency-selective time-varying channels, but also introduces interesting signal processing problems. One feature of the IEEE 802.16e OFDMA is the selectable discrete Fourier transform (DFT) or fast Fourier transform (FFT) size, from 128 to 2048 in multiples of 2, excluding 256 that is used in the OFDM PHY.

For each FFT size, the subcarriers are divided into three types: null (guard bands and DC), pilot, and data. A data stream can be carried over one or more subchannels depending on its rate. Three basic types of subchannel organization are defined: partial usage of subchannels (PUSC), full usage of subchannels (FUSC), and adaptive modulation and coding (AMC), among which PUSC is mandatory and the others are optional. In what follows, we focus on PUSC.

Figure 1 illustrates the structure of a time-division duplex (TDD) frame that only uses PUSC. The downlink (DL) subframe starts with a preamble, followed by $2n$ OFDMA symbols, and the uplink (UL) subframe contains $3m$ OFDMA symbols, where n and m are integers. The preamble is an OFDM symbol where the used subcarriers are spaced three indices apart and these subcarriers are BPSK-modulated with one of 114 selectable pseudo-noise (PN) sequences.

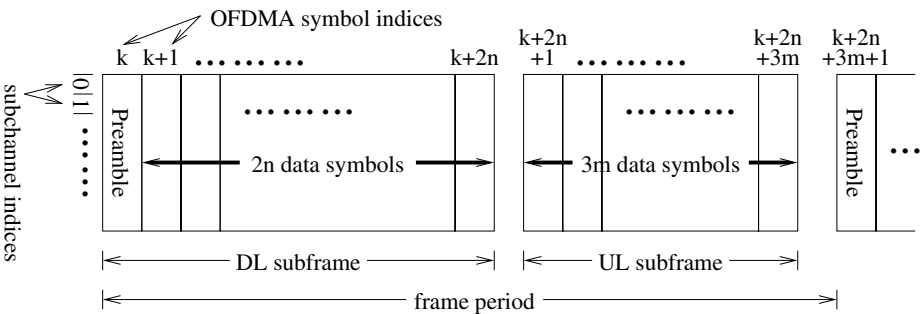


Fig. 1. Structure of IEEE 802.16e OFDMA TDD frame employing PUSC only

In the DL, every two successive OFDMA symbols form one unit in subchannel formation. Each subchannel consists of two “clusters” of subcarriers from each OFDMA symbol, where each cluster contains 12 data subcarriers and two pilot

2. Do channel estimation for the allocated UL burst locations of each SS.
3. Receive the signal from each SS in the allocated UL burst locations.

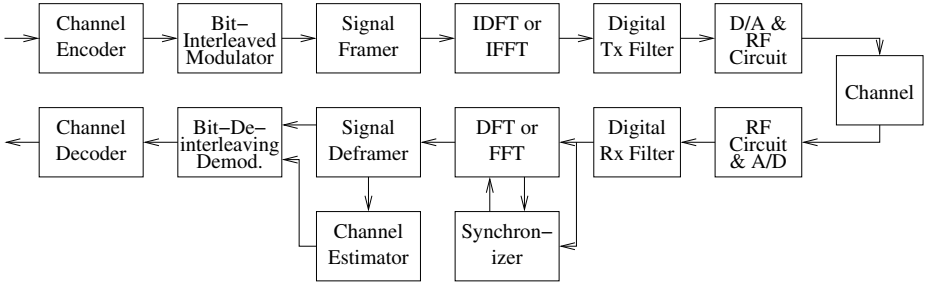


Fig. 4. Typical OFDMA transceiver structure

In the following, we discuss synchronization, channel estimation, and demodulation-decoding in separate subsections.

3.1 Synchronization

Consider initial DL synchronization first. In principle one can consider detecting the carrier frequency offset (CFO), the timing, and the preamble index jointly. But a less complicated approach is desirable for implementation purpose. Our method proceeds as follows:

1. In time domain, perform OFDMA symbol timing and fractional CFO estimation employing blind correlation based on the CP structure.
2. Convert the signal to frequency domain by FFT. Perform joint estimation of integer CFO and preamble index based on differential correlation.

After initial DL synchronization, we enter normal DL synchronization where we keep tracking of any variations in symbol timing and fractional CFO.

Let $r(k)$ be the received signal at time k , N be the FFT size, and L be the CP length. In step 1, the OFDMA symbol timing and the fractional CFO are estimated using the method in [2]:

$$\hat{\tau} = \arg \max_{\tau} \{ |\lambda(\tau)| \} , \quad \hat{\theta} = -\frac{1}{2\pi} \arctan \frac{\Im\{\lambda(\hat{\tau})\}}{\Re\{\lambda(\hat{\tau})\}} , \quad (1)$$

where

$$\lambda(\tau) = \sum_{k=\tau}^{\tau+L-1} r(k)r^*(k+N) . \quad (2)$$

In step 3, the differential received signal is given by

$$D_R[k] = \Re\{r(k)r^*(k+3)\} . \quad (3)$$

A differential sequence for each of the 114 preambles is also calculated, except that there is no need for the conjugation or the $\Re\{\}$ operation because the preambles are BPSK signals. Let $D_{ID}[k]$ denote the results, where $ID = 0, 1, \dots, 113$. Then $D_R[k]$ is correlated with each $D_{ID}[k]$ at each candidate integer CFO value. The combination of ID and integer CFO that yields the greatest correlation constitutes the estimator output. The above differential correlation method gives an approximate maximum-likelihood (ML) estimate in multipath channels [3].

In normal UL signal reception after the ranging process, only symbol timing and fractional CFO need to be synchronized. For this we employ the blind CP correlation as in step 1 of the initial DL synchronization.

3.2 Channel Estimation

In OFDM-type systems, channel estimates are needed for FEC decoding, among other things. A frequently considered channel estimation method in such systems is the simple least-square (LS) method that estimates the channel responses at pilot frequencies based on only one received OFDM or OFDMA symbol [4]. The estimates can be interpolated in frequency and in time to obtain channel estimates at non-pilot locations.

For OFDMA systems in slow fading, the received signal in frequency domain can be modeled as

$$r_k = H_k X_k + n_k \quad (4)$$

where k is the subcarrier index, H_k is the channel gain, x_k is the transmitted signal, and n_k is additive noise (assumed white Gaussian). An LS estimator minimizes the following squared error at the pilot locations:

$$\tilde{H}_k = \arg \min_{H_k} |r_k - H_k x_k|^2 . \quad (5)$$

With only one observed OFDMA symbol, the solution is simply

$$\tilde{H}_k = r_k / x_k . \quad (6)$$

Many frequency- and time-interpolation methods can be conceived [1]. The bilinear interpolation is one of the simplest. It is an appropriate choice when the frequency spacings of the pilot subcarriers are within a fraction of the coherent bandwidth and their temporal spacings are within a fraction of the coherence time. Such conditions are satisfied, for example, in both a DL cluster and a UL tile of an IEEE 802.16e OFDMA system of 10 MHz bandwidth, employing 1024-FFT, with carrier frequency below 3.5 GHz, and with mobile speed not over 120 km/h. When the channel response is subject to much slower time-variation, interpolation or averaging over a longer time period may be considered to yield more accurate channel estimates.

3.3 FEC Decoding

The mandatory coding scheme in IEEE802.16e OFDMA is tail-biting convolutional code (CC) with puncturing, followed by bit-interleaving and QAM. The

punctured bits can be treated as erasures in the CC trellis and thus do not affect the calculation of the path metrics. Both the tail-biting and the bit-interleaving influence the decoder design. We address them separately below.

Dealing with Tail-Biting. Tail-biting makes the encoder start in the state that it will end in. Optimal decoding of a tail-biting CC can be achieved by running as many parallel Viterbi decoders as there are states, with each decoder starting and ending in one different state. Then the best performer of all the decoder outputs gives the optimal solution. However, experience shows that conventional Viterbi decoding is easily a most complicated receiver function already. Since the code in IEEE 802.16e OFDMA has 64 states, the optimal solution is hardly practical for DSP implementation.

A suboptimal decoding method with good performance has been proposed [5], [6]. It employs only one Viterbi decoder that works on a circularly extended input sequence. The idea is that each path through the code trellis whose starting state and ending state are the same can be considered one cycle of an infinitely long periodic sequence. In Viterbi decoding, it is well-known that near-ML performance can be attained with a decoding delay of about 4 to 8 times the constraint length. Although we do not know the initial state of the received code sequence, if we perform Viterbi decoding long enough on the cyclically extended input sequence, we should converge to the optimal solution, but the leading segment and the trailing segment of the decoder output should be discarded.

Therefore, before decoding, we first do cyclic pre- and post-fixing of the received sequence for a sufficient length (e.g., both being 4–8 times the constraint length). After Viterbi decoding over the whole extended sequence, we drop the pre- and post-fixed segments to obtain the final decoder output.

Dealing with Bit-Interleaving. For ML Viterbi decoding in additive white Gaussian noise (AWGN), the error metric is the Euclidean distance between the trellis path and the soft-output of the demodulator. However, by having a bit-interleaver between the CC encoder and the QAM modulator, the combined trellis of the CC and the modulator becomes very entangled. As a result, the ML metrics become hard to calculate. A remedy is to approximate the path metric by the sum of bit metrics [7], [8]. A suitable bit metric for this is the log-likelihood ratio (LLR) [8]. The demodulator outputs the LLRs, which after bit-deinterleaving constitute the soft-decision inputs to the Viterbi decoder. For simplicity, log-sum approximation is applied to LLR calculation.

4 Simulation Results on Algorithm Performance

Table I lists the system parameters for many simulations reported below.

4.1 Synchronization

We report results on DL synchronization only. Let the transmission use a segment that is allocated 10 subchannels. Let the preamble index be 33, time offset be

Table 1. Parameters of simulated system

| Parameter | Value |
|---|---------------|
| Nominal Channel Bandwidth | 10 MHz |
| FFT Size (N_{FFT}) | 1024 |
| Subcarrier Spacing | 10.94 kHz |
| Useful Symbol Time (T_b) | 91.4 μ s |
| Guard Time ($T_g = 1/8 \cdot T_b$) | 11.4 μ s |
| OFDMA Symbol Time ($T_s = T_g + T_b$) | 102.9 μ s |
| No. of OFDMA Symbols per 5-ms Frame | 48* |

* 1 preamble + 12 \times 2 DL symbols + 7 \times 3 UL symbols + 2 gaps and unused time.

10 samples, and CFO be 9.35 subcarrier spacings. Two kinds of channel are simulated, namely, AWGN and the Stanford University Interim (SUI) [9].

Figure 5 shows the root-mean-square-error (RMSE) in symbol time estimation in AWGN. The floating-point results are obtained on personal computer (PC) and the fixed-point ones with Texas Instruments (TI)'s CCS tool for the TMS320C6416T DSP using 16-bit computation. Errors are small, and the performance difference between floating-point and fixed-point computations is little.

Figure 6 illustrates the RMSE in fractional CFO estimation in initial DL synchronization in the SUI3 channel at several mobile speeds up to 120 km/h. The RMSE is under 2% of the subcarrier spacing in medium to high signal-to-noise ratio (SNR). The performance in normal synchronization (not shown) is even better because more time has elapsed. The performance difference between floating-point computation and fixed-point computation is reasonable.

Finally, consider integer CFO and preamble index estimation, for which Fig. 7 shows some results for the SUI3 channel. The error rates are low.

4.2 Channel Estimation

We report results on DL channel estimation only, for UL results are characteristically similar. Consider transmitting in segment 0 with the 6 subchannels in “major group 0” allocated to it. Hence there are a total of 144 data subcarriers and 24 pilot subcarriers per symbol. Consider two fixed-point formats in 16-bit computation: Q3.12 and Q2.13. Figure 8 illustrates the mean-square error (MSE) in channel estimation under AWGN with QPSK modulation. The simulation results match well with theory, and the fixed-point results (obtained with CCS) are very close to that using floating-point computation. Figure 9 illustrates the MSE in channel estimation under SUI2 channel at 60 km/h speed. We see that the Q2.13 data format has sufficient dynamic range and, by having one more fractional bit than Q3.12, shows a lower error floor in high SNR.

4.3 FEC

Seven combinations of modulation and coding schemes are defined in the tail-biting CC mode of IEEE 802.16e OFDMA. Figure 10 illustrates the bit error rate

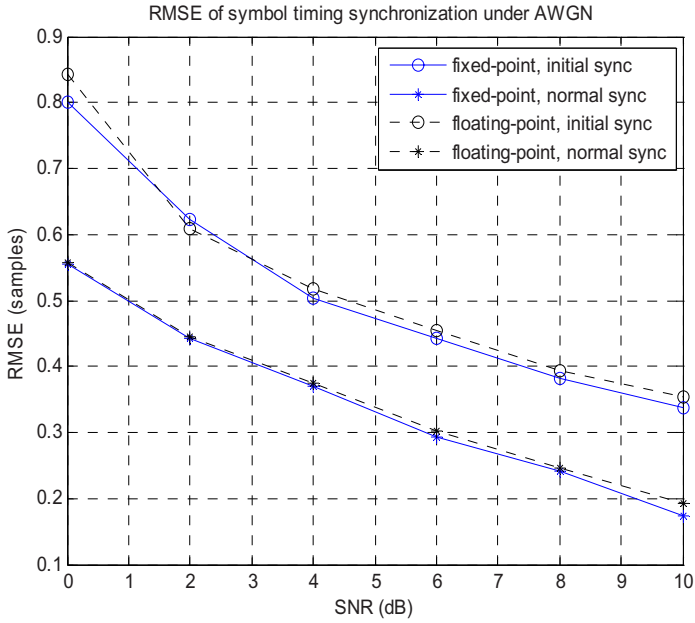


Fig. 5. Performance of symbol time estimation in AWGN

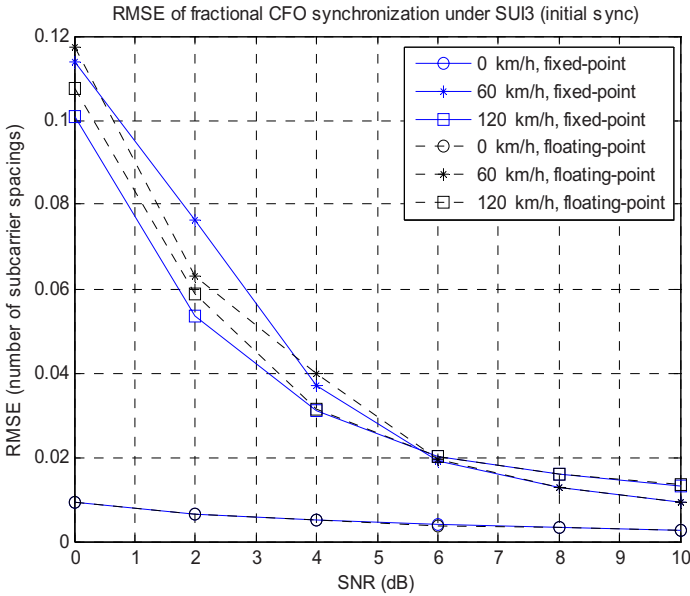


Fig. 6. Performance of fractional CFO estimation in initial DL synchronization in SU13 channel

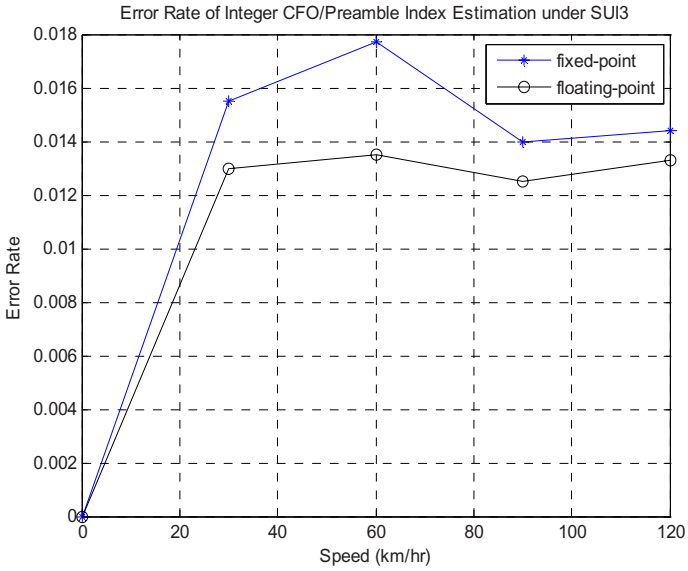


Fig. 7. Performance of integer CFO and preamble index estimation in SUI3 for mobile speed up to 120 km/h

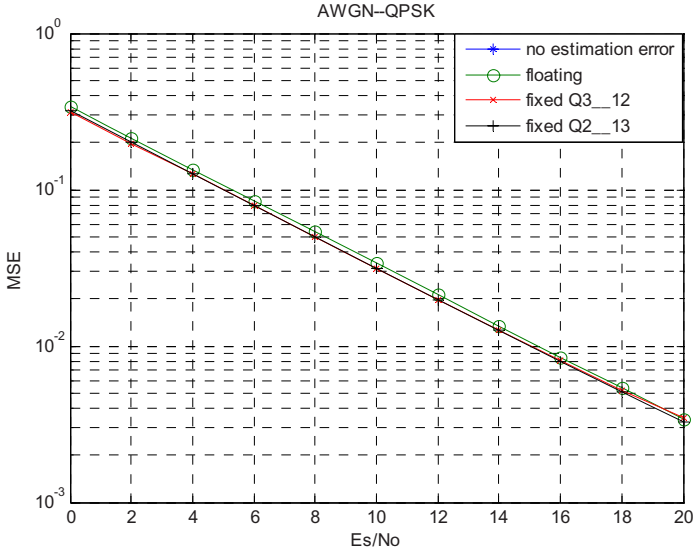


Fig. 8. MSE of DL channel estimation under AWGN

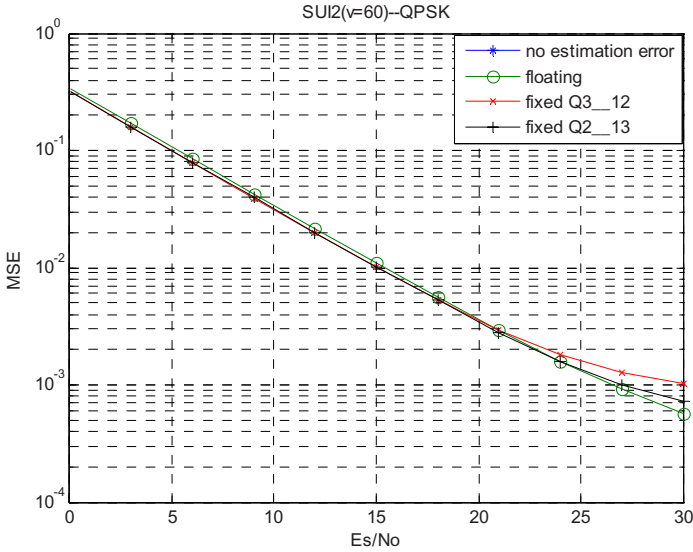


Fig. 9. MSE of DL channel estimation under SUI2 channel at mobile speed 60 km/h

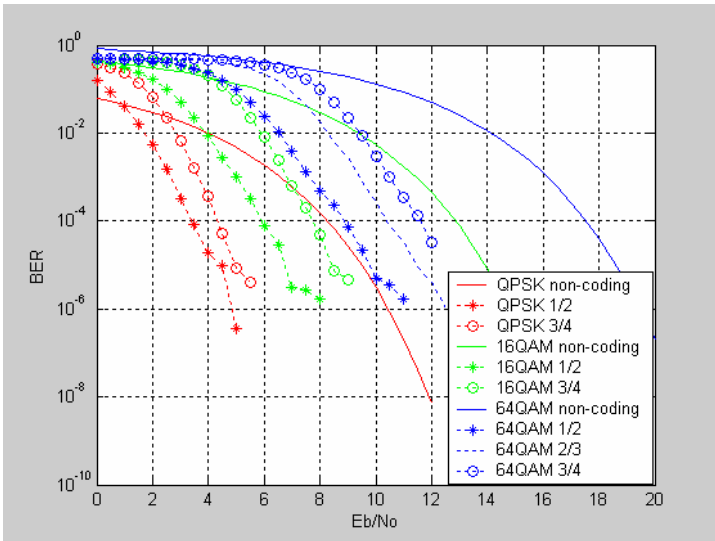


Fig. 10. FEC performance with fixed-point computation

(BER) performance of FEC decoding in AWGN with fixed-point computation, where the number after each modulation type in the legend denotes the code rate. For space reason, we omit a plot of the results with floating-point computation. Suffice it to say that they are in good correspondence.

5 DSP Software Implementation

For DSP implementation, we employ Sundance’s SMT8096 platform which is built around TI’s TMS320C6416T DSP. The SMT8096 comprises of an SMT310Q PCI PC plug-in board called a “carrier” which can house four SMT395 daughter cards termed Texas Instruments Modules (TIMs). Each TIM houses one TMS320C6416T DSP. The DSP contains 8 parallel function units and runs at 1 GHz. Two TIMs can communicate through the Sundance Digital Bus (SDB). The PCI interface of SMT310Q runs at 33 MHz with a 32-bit data bus. The DSP platform employs the 3L Diamond real-time operating system that supports multiple processor communication and synchronization.

Table 2. Computational performance of the implemented system

| Module | DSP Computational Load* |
|-------------------------------------|-------------------------|
| Baseband Transmitter exc. Tx Filter | 0.82 |
| Tx Filter (4× oversampled) | 0.25 |
| Channel Simulators: | |
| AWGN | 0.82 |
| SUI | 1.52 |
| ETSLA | 2.56 |
| Rx Filter (4× oversampled) | 0.54 |
| FFT, Sync., & Channel Estimation | 0.23 |
| Deframing, Demod., & Decoding | 1.16 |

* As multiple of one DSP’s computational capability.

For processing speed and convenience in work division, four TIMs are used: one for the transmitter functions, two for the receiver functions, and one to simulate the equivalent lowpass wireless channel. Table 2 shows the computational speed of the integrated implementation for a 10-MHz bandwidth, 1024-FFT system in DL transmission. Note that channel decoding is a most computation-intensive transceiver function. But interestingly, some “basic” functions, such as the transmitter and the receiver filters, also require much computation. Comparatively, the proposed synchronization and channel estimation methods are less computation-intensive, but they have significant impact on the transmission performance and require a careful design.

6 Conclusion

We considered the OFDMA PHY of the IEEE 802.16e standard and discussed the design of some key signal processing functions. We described a fully software implementation of these functions employing Texas Instruments’ DSPs. Acknowledgeably, the implementation still has much room for improvement. However, it demonstrates that a fully software implementation of the baseband transceiver functions for a system as complicated as the Mobile WiMAX is not

beyond reach. In addition, such an implementation is a useful tool that can serve various research, prototyping, and functional verification purposes.

Acknowledgments. This work was supported by the New Generation Broadband Wireless Communication Technologies and Applications Project of the Institute for Information Industry, sponsored by MOEA, R.O.C., under Grant 96-EC-17-A-03-R7-0765 and by the National Science Council of R.O.C. under Grant 95-2219-E-009-003. The following people also played a major role in the reported work: Soon Seng Teo, Yao-Chun Liu, Yi-Ling Wang, and Po-Sheng Wu.

References

1. Hung, K.-C., Lin, D.W., Lee, Y.-T., Loa, K.: WirelessMAN physical layer specifications: signal processing perspective. In: Zhang, Y., Chen, H.-H. (eds.) *Mobile WiMAX: Toward Broadband Wireless Metropolitan Area Networks* Ch. 3, Auerbach (2007)
2. Lin, J.-C.: Maximum-likelihood frame timing instant and frequency offset estimation for OFDM communication over a fast Rayleigh fading channel. *IEEE Trans. Veh. Technol.* 52, 1049–1062 (2003)
3. Hung, K.-C., Lin, D.W.: Joint detection of integral carrier frequency offset and preamble index in OFDMA WiMAX downlink synchronization. In: *IEEE Wireless Commun. Networking Conf.*, pp. 1961–1966 (2007)
4. van de Beek, J.-J., Edfors, O., Sandell, M., Wilson, S.K., Börjesson, P.O.: On channel estimation in OFDM systems. In: *IEEE 45th Veh. Technol. Conf.*, vol. 2, pp. 815–819 (1995)
5. Wang, Y.-P.E., Ramesh, R.: To bite or not to bite — a study of tail bits versus tail-biting. In: *Proc. IEEE Int. Symp. Personal Indoor mobile Radio Commun.*, vol. 2, pp. 317–321 (1996)
6. Sung, W., Kim, I.-K.: Performance of a fixed delay decoding scheme for tail biting convolutional codes. In: *Proc. IEEE Asilomar Signal Syst. Computers Conf.*, vol. 1, pp. 704–708 (1996)
7. Zehavi, E.: 8-PSK trellis code for a Rayleigh channel. *IEEE Trans. Commun.* 40, 837–884 (1992)
8. Tosato, F., Bisaglia, P.: Simplified soft-output demapper for binary interleaved COFDM with application to HIPERLAN/2. In: *IEEE Global Telecommun. Conf.*, vol. 2, pp. 664–668 (2002)
9. Erceg, V., et al.: Channel models for fixed wireless applications. Standards contribution no. IEEE 802.16.3c-01/29r4 (2001)

Cross-Layer Design for IEEE 802.16-2005 System Using Platform-Based Methodologies

Li-chuan Tseng, Kuan-yin Chen, and ChingYao Huang

Institute of Electronics, National Chiao-Tung University, Hsinchu, Taiwan
{lctseng.ee90, cgi0911.ee94g}@nctu.edu.tw
<http://wintech.ee.nctu.edu.tw>

Abstract. In this article, we present a cross-layer design scheme for 802.16-2005 system. The cross-layer design includes both MAC and PHY and is implemented through platform-based methods. In this design, we discuss how the cross-layer design affects radio resource management efficiency and system timing by examining system throughput. As for the platform-based design, we present a method that enables designers to estimate the allocation of hardware costs at an early design stage.

Keywords: IEEE 802.16, Platform-Based Design, Cross-layer, HW/SW Co-Design, Performance Estimation.

1 Introduction

As the demand of broadband wireless access (BWA) grows rapidly, people need new standards to provide high speed wireless transmission services. The OFDMA-based IEEE 802.16-2005 Standard (Mobile WiMAX) has become the most important candidates among all cellular technologies supporting BWA services. However, the system design becomes more challenging with higher system performance requirement. Designers are seeking for new design approaches to overcome strict constraints such as a standby time, hardware size, and etc.

With suitable architecture and optimal performance, our research objective is to discover new design approaches for the ratified Mobile WiMAX Standard [1] [2]. An example of system architecture was discussed in [3]. Algorithm design and performance simulation issues were discussed in [4].

An important issue for communication system implementation is the layer structure. Traditionally, a layered model such as OSI 7-layer structure separates the whole system into well defined layers. This is to facilitate system development, and provide compatibility between products from different vendors. In traditional layered designs, direct communications between layers are forbidden, only procedure calls and responses are allowed [5].

However, for modern high-speed BWA systems, the traditional approaches become an obstruction for designers to meet strict performance criteria. Lack of instant RF information in upper layers causes inefficiency of radio resource management (RRM), while procedure calls and responses bring unnecessary execution overheads. In view of this, designers began to choose cross-layer design

strategies, aiming to break inter-layer boundary and to enhance communication among layers. Many studies such as [5] [6] provide a theoretical view of cross-layer design.

In our studies, we define a reduced system architecture, and try to implement the system including MAC and PHY layers. The design and implementation of advanced MAC and PHY layers in mobile communication is challenging. Undoubtedly, the PHY layer functional blocks are mostly implemented as hardware (possibly on DSP). For the MAC part, since the functions become more complex, a pure-software design is not adequate, thus we need to partition the system into hardware and software parts. Traditionally, we design hardware part with FPGA and then port the software part onto the system such as [7] [8]. Now we are able to design HW and SW parts simultaneously with a platform-based strategy, in which the HW part can be modeled at the transaction level using systemC. This method significantly facilitates the software design since software can now be developed in parallel with hardware just after the hardware modules are defined. This also helps us to have better insight on the whole architecture and protocol issues.

The rest of the paper is organized as follows: First, we provide an overview of the WiMAX standard in Section 2. In Section 3, some cross-layer design issues are discussed. In Section 4, the proposed architecture for the MAC and PHY layer system are described. Section 5 includes a hardware-software co-design example and simulation results. Finally, conclusions are drawn in Section 6.

2 802.16-2005 MAC and PHY Overview

MAC Layer - The MAC layer of Mobile WiMAX can be roughly separated into two planes, data plane and control plane, according to the functionality [1] [2]:

A. Data Plane

Data plane is responsible for forming protocol data units (PDU) from data packets, i.e. service data units (SDU) coming from upper layers. Construction of the data plane is based on the data flow between upper layers and the PHY layer, which can be classified into following steps:

- **Convergence Sublayer**
including Packet Header Suppression (PHS) and Packet Classification. The packet classifier maps packets into various connections according to its service flow.
- **Fragmentation and De-fragmentation**
For connections without ARQ support, the SDUs are subjected to further fragmentation and packing. For connections with ARQ support, the SDUs are reduced to fixed-sized blocks and are not apt for further changes.
- **Header and Subheader**
Headers and subheaders are appended to payload according to its contents and properties or control messages in between BS and MS.

- **CRC Computation**
CRC field is generated for error detection. This is optional in IEEE 802.16-2004 but mandatory in 802.16-2005.
- **Framing**
The PDUs are collected and concatenated, i.e. PDUs are packed into data bursts according to their destination.
- **Interaction with Control Plane**
Another source of PDU payloads are management messages. The decision of message parameters is in the control plane, while the data plane is responsible for accessing the parameters and turns them into PDU payloads. This takes complicated bit manipulations.

B. Control Plane

- **Mobility Control**
This part handles mobility issues of MSs, such as motion, switching among multiple cells, and power adjustments. This part includes the following functional blocks:
 1. Cell Reselection and Handover.
 2. Idle Mode and Sleep Mode.
 3. Active Mode Power Management.
 4. Channel Measurement.
- **Network Entry**
Network entry part in Mobile WiMAX is responsible for initializing network connection between MS and BS. It is also responsible for handling new network entries if MSs wish to handover from one network to another.
- **Scheduling**
The system will arrange transmission order among SDUs of different connections according to scheduling rules. Scheduling algorithms vary in accordance to different QoS classes.
- **Management Message Composer**
The parameters needed in a management message are gathered by the composer, and then passed to the data plane in the form of C language structure.

PHY Layer - The mobile WiMAX system has an OFDMA-based physical layer:

- **IFFT / FFT**
The kernel of OFDM, also the part that occupies most hardware resources in PHY implementation.
- **Interleaving and randomization**
To combat the burst error problem of time-varying wireless channel
- **Channel coding and digital modulation**
PHY encodes and modulates the signal to reflect the changes of link performance
- **Synchronization and Channel Estimation**
implemented at the receiver side with the help of preamble and MAC management messages

3 Cross-Layer Issues

As discussed in [5] [6], the cross-layer control and optimization strategy can be categorized into several classes. For example, top-down approach, in which the lower layer is controlled by a higher layer; feedback approach, which is top-down controlled with some information feedback from the lower layer; integrated approach, in which two or more layers are considered together. While we have several choices for each layer, an optimization task is setup to find a jointly optimal solution. The following part describes some issues that need cross-layer solutions:

A. Radio Resource Management

The MAC layer makes decisions on many functions: scheduling, handover triggering, power control, coding-modulation scheme selection, etc. These decisions require PHY layer measurements such as CINR, RSSI, BER, and others. In many circumstances, layered signaling is just not efficient enough for radio resource allocation. Reference layered structure passes parameters layer-by-layer and simply takes too much time, so that signaling contrarily becomes a bottleneck for high-speed MAC design. In view of this, new interfaces shall be added between adjacent layers, and even non-adjacent layers to provide a quicker runtime signaling.

B. Performance Considerations

As the system become more complex, cross-layer signaling is no longer as simple as connecting adjacent layers. The interface must be efficient enough so that overhead is minimized and thus can provide high speed and high throughput. In mobile WiMAX, this is partially done by MAC management messages parameters defined in the protocol. However, the actual passing of parameters and data stream, through hardware pins or software variables, still needs to be designed carefully.

To solve the problems stated above, we will examine the problems from the architecture point of view. The main idea is that for those functional blocks which are closely interacted should be designed as an integrated module. Some examples are:

- **Framing**

Framing includes selection of the coding-modulation scheme and bit-loading. These are conventionally categorized as MAC functions. FEC encoding and modulation are categorized as PHY functions. These functional blocks comprise the kernel of data transmission. In conventional layered structure, the MAC layer constructs a complete frame including several data bursts and necessary control fields, such as FCH and DL/UL-MAPs. After that, the MAC layer passes the whole frame to PHY layer in the form of bit-stream. However, we shall show the problem of execution overhead in the later parts of this article.

– Ranging/Handover

In ranging or handover processes, a device detects the environment to adjust its transmission parameter or switch to another base station. They both include the cross-layer signaling that the channel condition (CINR or RSSI) is passed from PHY to MAC, and control information (e.g. power adjustment, HO command) is passed from MAC to PHY. The measurements and parameters passing can be more efficient if we design specific connections among related functional blocks.

4 System Architecture

A. Proposed System Architecture

Fig.1 is our proposed system architecture with cross-layer consideration, for the transmitting function of a base station (BS). The architecture includes two planes, the data plane and the control plane. Two planes are linked together by a public parameter database.

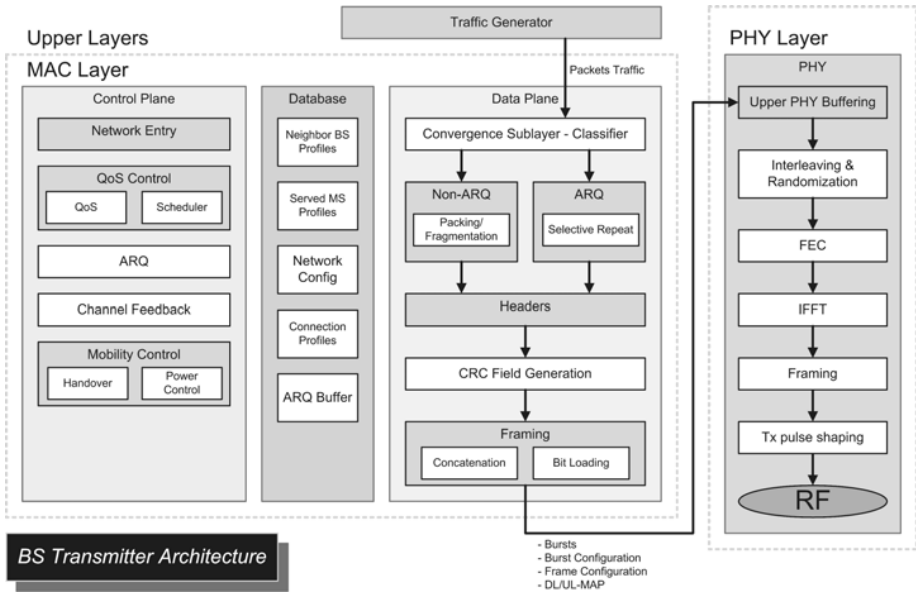


Fig. 1. Proposed System Architecture

The data plane is based on the data flow between upper layers and the PHY layer, with separated flows for ARQ and non-ARQ connections. The control plane is classified into various blocks according to functionality. Between the two planes there is a shared database. Parameters, BS/MS profiles and network configuration profile are stored in the database. Control plane message composer,

data plane, and algorithm modules will access the shared database. The receiver side is roughly the inverse of the transmitting one, except that the PHY part should be a little more complex to include synchronization and channel estimation. Receiver architecture is not discussed in this article.

B. Modulized Algorithm Development

To facilitate algorithm development, the algorithm functional blocks must be fully modularized and can be easily added or removed. This can be done by applying a standard interface, as illustrated in Fig. 1. The standard interface comes in the form of a variable database, accessed by all algorithm modules, message composer and data plane. If necessary, new variables and algorithm modules can be added at ease.

5 Design and Implementation Issues

A. Design Flow

We implement the 802.16-2005 MAC and PHY layers in a platform-based ESL (Electronic System Level) design manner. The complete design progress starts from defining or understanding system specification, based on this, we have an architecture containing functional blocks with control and data signal flows. Then we implement the system with both hardware and software and then verify the design at final. The proposed design flow is described in Fig. 2 and will be explained as follows.

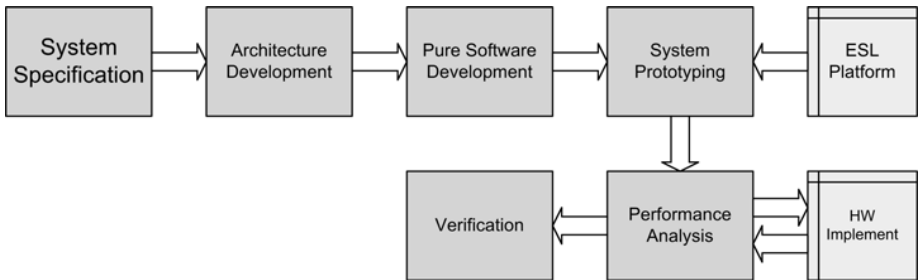


Fig. 2. Proposed System Design Flow

To have a system view at a higher level, it is preferred to implement the system with pure software from the start. Algorithm development and layer interface issues are handled at this stage. We apply profiling in order to gain a rough insight of system performance, and then considering the cross-layer co-simulation in order to ensure the function correctness.

After software development, to facilitate real-time operation, substitution of bottleneck functional blocks with HW implementation is a necessary means. For

our communication system case, the PHY layer baseband processing is hardly to be kept in software due to its high computation power, so it will be transfer into a hardware model and than implemented with specific hardware architecture. The MAC data plane, especially the part dealing with SDUs, also contains computational operations that is routined and repeated, and is therefore more favorable for HW substitution. The control plane, which contains less frequently called functions and each requires variable amount of memory, is less favorable.

Note that the implementation of pure software does not need to have a complete control plane. An important benefit of ESL design is that the hardware and software can be developed simultaneously. This means, using hardware "models" with well-defined interfaces, we may refine the software without actual implementation (FPGA or ASIC) of hardware part. Take the scheduler as an example, we may use a simple FIFO queue at the beginning (in order to verify the hardware model), and applying more complex algorithms later.

In the example presented in Section 6, HW/SW co-simulation is done by building a processor based platform. The design tool used for platform construction is the ARM RealView SoC designer; like other similar tools, there is a canvas to draw a platform and simulate it.

B. Effect of Cross-Layer Design on Timing

Besides radio resource issues, cross-layered design may bring great influence on hardware timing. In traditional discrete-layered designs, MAC and PHY threads are executed separately. The two layers are connected only through buffering and signaling. Only after the procedure of one layer is completed, it will then issue a procedure call and start another layer's procedure. However, buffering and signaling bring excessive memory accesses, which is the main reason for system throughput degradation. If a designer wishes to solve this problem, it would be better if the procedure sequence is re-arranged. By merging MAC and PHY layer into an optimized hardware module, we are able to reduce excessive memory accesses and thus improve system timing.

Here is an example illustrating how hardware timing is improved by merging both layers. Consider the sequential execution of packing- fragmentation, which is a function of MAC data plane, and then FEC encoding and modulation, which belongs to PHY layer. The sequence's goal is to generate data for n bursts, and then propagate these bursts through FEC coding and modulation.

Three execution schemes are examined:

- A. Discrete-layered execution, without any hardware optimization.
- B. Discrete-layered execution, with all PHY functions integrated into a hardware module.
- C. Cross-layered execution, with MAC and PHY functions integrated into a single hardware module.

For scheme A and B, the execution sequence can be expressed by the following pseudo code:

```

MAC_Procedure()
{
    for( i <= n_burst )
        while( burst[i] is not full )
            fragmentation/packing();

    PHY_Procedure ();
}

PHY_Procedure()
{
    retrieve_MAC_parameters();
    upper_PHY_buffer();

    for( i <= n_burst )    FEC_encoding( burst[i] );
    for( i <= n_burst )    Modulation( burst[i] );
}

```

For scheme C, the pseudo code expression is:

```

Integrated_Procedure()
{
    for( i <= n_burst )
        while( burst[i] is not full)
            fragmentation/packing();

    retrieve_MAC_parameters();

    FEC_encoding( burst[i] );
    Modulation( burst[i] );
}

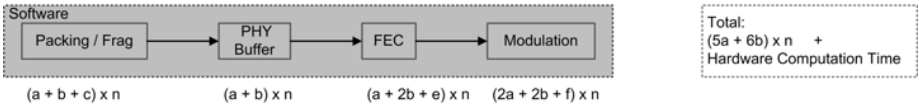
```

From the pseudo codes, we observe that in scheme A and B, there are three loop structures that each of them has n iterations, thus giving $3n$ conditional branches. In scheme C, there is only one loop structure, giving n conditional branches. Under massive amount of loop execution, this could bring obvious performance difference.

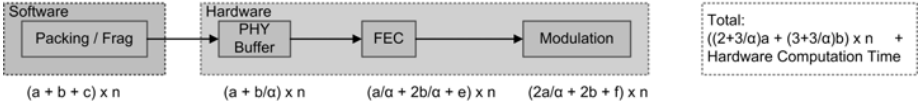
Also to quickly estimate system performance, we model the system's memory access behavior with the following assumptions:

- Time needed for reading a burst's bit load from system RAM, denoted by a .
- Time needed for writing a burst's bit load to system RAM, denoted by b .
- Time needed for reading a burst's bit load from hardware cache, denoted by a/α . Note that α is the average speedup ratio between system RAM and hardware cache access.
- Time needed for writing a burst's bit load to hardware cache, denoted b/α .
- Number of bursts, denoted by n .
- Computation time for packing/fragmentation, FEC encoding and modulation respectively, denoted by c , e and f .

Scheme A: Discrete MAC and PHY Design without HW Optimization



Scheme B: Discrete MAC and PHY Design with PHY HW Optimization



Scheme C: MAC and PHY Cross-Layered Design with Integrated HW Optimization



Fig. 3. Execution Sequence and Memory Access Time Estimation for Three Schemes

Note that a burst’s bit load would increase through FEC encoding. Here we assume the code rate is 1/2, and therefore the bit load after FEC process is double of that before encoding. Also we focus on memory access time in this part; the acceleration within each functional blocks, i.e. changes in execution time c , e and f are NOT considered.

Refer to Figure 3, we can derive approximate memory access time for each execution scheme, shown as follows:

- Scheme A: $(5a + 6b) \times n$
- Scheme B: $((2+3/\alpha)a + (3+3/\alpha)b) \times n$
- Scheme C: $((1+3/\alpha)a + (2+3/\alpha)b) \times n$

Since the access speed of hardware cache is much faster than that of system RAM, we can assume that α has a large value, and therefore we have further approximation shown as follows:

- Scheme A: $(5a + 6b) \times n$
- Scheme B: $(2a + 3b) \times n$
- Scheme C: $(a + 2b) \times n$

From the estimation stated above, hardware integration of MAC and PHY can dramatically reduce memory access time by almost 75%, thus improve system throughput.

B. Predict HW behavior with HW/SW Partition

The most exciting advantage of platform-based design is that we can develop hardware and software part simultaneously after a proper interface is defined

by rough software and some hardware models. However, the interface can still be defined without this platform-based simulation, so why do we need it? The answer is that it provides us with more precise information of hardware behavior, including ports, cycle count, before actual hardware tape-out. But some information, like the cycle-accurate hardware execution time, is still unavailable until Verilog designs are completed. If a designer needs to know more about the performance evaluation in the early stage, a systematic way should be developed.

We formulate this problem with the following factors:

For the system before HW/SW optimization, we have:

- C_{Si} : Software execution cycle count of the i^{th} functional block, per instance.
- U_i : How many times the i^{th} functional block is referenced.

B. After HW/SW optimization, we have:

- C_H : Target total cycle count of all hardware modules.
- C_{Hi} : Cycle count of the i^{th} functional block, after it is implemented with hardware.

The designer sets up a fixed goal for C_H according to the timing constraint, and then allocates a target C_{Hi} value for each functional block which will be implemented with hardware. The goal is now to find out a combination of C_{Hi} values that minimizes the system cost, say hardware area, under a fixed constraint of total C_H .

Here we introduce another factor, γ_i , which is a characterization factor of the i^{th} functional block. The factor indicates how easy the functional block could be boosted with a compact sized hardware implementation. As an example, functions such as FFT and IFFT can be accelerated with Butterfly structure, which is relatively small in size. Therefore they have higher γ_i values.

Then the *cost function* can be defined as:

$$J' = \sum_i \frac{C_{Si}}{\gamma_i C_{Hi}} \quad (1)$$

J' has the same trend with required hardware area, and therefore is a good indicator of hardware area needed for the functional block.

Our goal is to minimize J' , subject to the constraint

$$\sum_i C_{Hi} U_i \leq C_H \quad (2)$$

where C_H is a fixed target, we solve the optimization problem of minimizing J' with Lagrange Multiplier Method, shown as follows:

$$J = J' + \lambda \left(\sum_i C_{Hi} U_i - C_H \right) \quad (3)$$

where λ is the Lagrange Multiplier. We seek for the minimum value of cost function by taking partial derivation with respect to C_{Hi} , and let it equal to zero:

$$\frac{\partial J}{\partial C_{Hi}} = -\frac{C_{Si}}{\gamma_i C_{Hi}^2} + \lambda U_i = 0 \quad (4)$$

Solving equation 4, we have:

$$C_{Hi}^2 = \frac{C_{Si}}{\lambda \gamma_i U_i} \quad (5)$$

from which we can allocate each functional block an adequate target cycle count, and minimize the corresponding hardware area cost. This is a reasonable allocation since:

- For a functional block which costs more software cycle originally, we allocate more hardware cycle.
- For a functional block which is used more frequently, we allocate less hardware cycle to reduce the overall hardware cycle, at the expense of increasing area or power.

With similar procedures, designers are also able to compute the allocation of hardware resource subjected to other criteria such as hardware power.

Here we consider a simplified implementation of WiMAX MAC and PHY layers. The pure software version needs about 14.6 M cycles to complete a frame, which equals to 146ms with a fully utilized processor running at 100 MHz. This is the estimation result without any aid of application-specified hardware or DSP modules, and is much higher than the standard-specified 5ms goal. Therefore, designers have to consider optimizing some functional blocks with hardware.

According to the estimation method described in equation 1 to 4, Table 1 shows the profiling results of two heavy loaded modules, IFFT and FEC Encoder, and their corresponding parameter settings. A simulation period of 20 frames is applied.

Table 1. Profiling Result

| Function | U_i | C_{Si} | γ_i |
|-----------------|-------|----------|------------|
| (1) IFFT | 660 | 313511 | 5 |
| (2) FEC Encoder | 320 | 192995 | 1 |

Setting $C_H = 600,000$ cycles allows the frames to be generated on time (processor not fully-used). Using equation 2 and 5, we allocate $C_{H1} = 400$ cycles, and $C_{H2} = 1000$ cycles.

6 Conclusion

In this paper, we presented a cross-layer design methodology of Mobile WiMAX MAC layer, involving both hardware and software designs. By combining MAC

and PHY layer, designers are able to reduce excessive memory access and looping, thus improve system performance. Also, in a HW/SW co-design platform, we can allocate target cycle counts for each HW component according to some rules so that the cost is minimized.

Acknowledgment

This work is sponsored by Institute for Information Industry, Taiwan.

References

1. IEEE Standard for local and metropolitan area networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std. 802.16 (2004)
2. IEEE Standard for local and metropolitan area networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE Std. 802.16 (2005)
3. Kwon, T., et al.: Design and Implementation of a Simulator Based on a Cross-Layer Protocol between MAC and PHY Layers in a WiBro Compatible IEEE 802.16e OFDMA System. *IEEE Commun. Mag.*, 136–146 (December 2005)
4. Settembre, M., et al.: Performance Analysis of an Efficient Packet-Based IEEE 802.16 MAC Supporting Adaptive Modulation and Coding. In: *Proceedings of the Seventh IEEE International Symposium on Computer Networks* (2006)
5. Srivastava, V.: Cross-Layer Design: A Survey and the Road Ahead. *IEEE Communications Magazine* (2005)
6. Wang, Q., et al.: Cross-Layer Signaling for Next-Generation Wireless Systems. In: *WCNC 2003. Wireless Communications and Networking* (2003)
7. Holisaz, H., et al.: Hardware Accelerator IP-Core for Wireless 802.16 MAC. In: *IFIP International Conference on Wireless and Optical Communications Networks* (2006)
8. Sung, N.W.: HW/SW Co-designed Implementation of IEEE 802.16 TDMA MAC for the Subscriber Station. In: *Proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science* (2005)

A Dynamic Frequency Allocation Scheme for IEEE 802.16 OFDMA-Based WMANs Using Hungary Algorithm

Shiann-Tsong Sheu, Chih-Chen Yang, and Hsu-Sheng Chang

Department of Communication Engineering, National Central University, Taiwan, R.O.C.
stsheu@ce.ncu.edu.tw

Abstract. In IEEE 802.16 Wireless Metropolitan Area Networks (WMAN) with Orthogonal Frequency Division Multiple Access (OFDMA) physical layer, dynamic subchannel allocation algorithm (DSAA) is essential for a Base Station (BS) to efficiently utilize bandwidth capacity. Conventional DSAs usually group all subcarriers into a number of subchannels and allocate subchannels to Subscriber Stations (SS), one for each SS, according to its traffic demand and channel quality of the link between BS. However, the restriction of conventional DSAs allocating N subchannels to N SSs ($N \geq 1$) is inflexible and inefficient with respect to spectrum efficiency. In this paper, a new DSAA with Hungary algorithm is proposed to enhance the subchannel capacity (in bits per subcarrier) by permitting more than one subchannel allocated for one SS for which channel quality is much better than others.

Keywords: Dynamic Frequency Selection, Hungary Algorithm, Orthogonal Frequency Division Multiple Access (OFDMA), WMAN.

1 Introduction

The basic concept of Orthogonal Frequency Division Multiple Access (OFDMA) is to make use of OFDM modulation and allow multiple-access by dividing the whole subcarriers into a number of subchannels, which are the granular units for allocating to Subscriber Stations (SSs). Nowadays, the OFDMA system adopted by the IEEE 802.16 Mobile Wireless Metropolitan Area Network (M-WMAN) standard becomes one of the most important broadband wireless technologies.

With Orthogonal Frequency Division Multiplexing (OFDM) system, SSs use all data subcarriers of a channel to transmit data frames. However, it is hard to guarantee every SS always transmits with good channel condition. Contrarily, in OFDMA system, all data subcarriers are flexibly grouped to form a number of subchannels and one SS may be assigned to use more than one subchannel (i.e. partial subcarriers of a channel form the system viewpoint) to transmit data frames with the other SSs which are assigned to use different subchannels simultaneously. All subchannels have to be assigned to SSs in an exclusive manner. If some subchannel is assigned to improper user, the poor channel condition between BS and that user resulted from deep channel

fading on some parts of subcarriers will degrade the transmission reliability. A smartly dynamic frequency allocation scheme should assign every subchannel to the SS which has the best channel condition with respect to that subchannel. As a result, the subchannel allocation according to the channel conditions of SSs makes SSs to transmit data frames using a more aggressive modulation and coding scheme. The issue becomes how to allocate all subchannels to SSs appropriately. Many algorithms have been proposed to resolve this issue. In paper [1], authors have proposed an iteration method to change the static allocation method to be the dynamic allocation method. The simulation results showed that it indeed increases the system capacity and decreases the bit error rate (BER) for the environments with same signal-to-noise ratio (SNR). However, the probability of making successful allocations is only 76.5% if there are 16 subchannels. In paper [2], a dynamic frequency selection is proposed to modify the method to improve the performance of the system and the successful probability of subchannel allocations. The proposed algorithm divides the subcarriers into a large number of subchannels and provides each SS one or more than one subchannel depending on the channel conditions. However, with the proposed algorithm, the number of available subchannels to be allocated to each SS must be given first. Due to this reason, one SS may be allocated to use the subchannels which might be more suitable for the other SS. So, the restriction of the given number of subchannels per SS limits the flexibility of subchannel allocations and the spectrum efficiency. Obviously, the proposed algorithm is not flexible enough and there are some shortcomings we should resolve.

To optimize the system performance, the algorithm ‘Hungary Algorithm’ (HA) [3] designed for the task assignment is adopted to derive the optimal subchannel assignment in this paper. We also amend HA to have the ability of flexibly assigning different numbers of subchannels to SSs according to the channel conditions of SSs

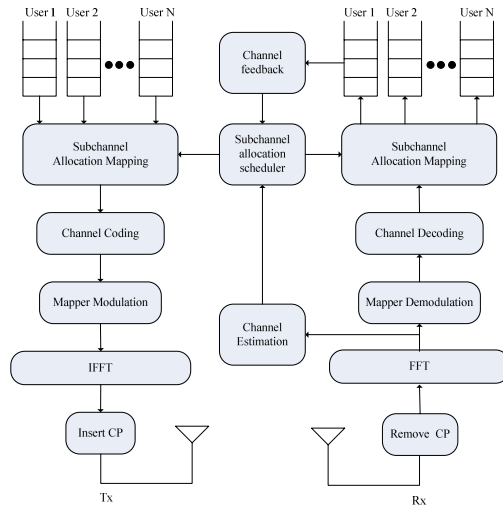


Fig. 1. System model for OFDMA system with subchannel allocation scheduler

from time to time. Simulation results show that the proposed algorithm performs better than previous ones in terms of bit error rate (BER) under the same signal-to-noise ration (SNR) environment.

The paper is organized as follows. Section 2 shows the OFDMA system model considered in this paper. The proposed algorithm is introduced in Section 3. Simulation results and conclusions are presented in Section 4 and Section 5 respectively.

2 System Model

The OFDMA system block diagram of BS is showed in Figure 1. Let N denote the number of SSs in the system, and BS allocates data queues for SSs, one for each. Subchannel allocation scheduler is required to allocate suitable subchannels to SSs in order to increase the probability of successful frame transmissions.

As radio signal is received by the receiver of BS, the cyclic prefix is removed first and then the signal is transformed by using Fast Fourier Transform (FFT). After then, receiver side does the channel estimation for retrieving the usefully channel condition of each subchannel to the sender SS. Next, the transformed signal is demodulated and decoded according to retrieved channel condition. Finally, subchannel allocation mapping would separate data frames from signal and put data frames to the right queues according to the subchannel allocation decision made by subchannel allocation scheduler. In data frames, there could have some channel feedback information from SSs, and such information is passed to the subchannel allocation scheduler to be the important reference for deciding subchannel allocations.

3 Dynamic Frequency Allocation

3.1 Conventional Algorithms

The simplest allocation algorithm is 'static allocation' algorithm. With this allocation algorithm, the whole subcarriers are divided into several subchannels and each subchannel is allocated to a SS by given order regardless of channel condition. However it is not an allocation algorithm to optimize the system throughput. In paper [1], the whole subcarriers are also divided into several subchannels but each subchannel is allocated to a SS who has the highest channel gain in the subchannel. By this way, the number of subchannels should be equal to the number of SSs. However, it is not a good allocation algorithm because the subchannels are assigned without considering the channel condition. Furthermore, two SSs might be chosen to use the same subchannel to transmit because of the same channel gain. For such situation, paper [2] proposes a method to solve the conflict. Let $U_{N(t-1)}$ denote the usage factor of subchannel N during the previous iteration, say $t-1$, C_N denote as the cost of using subchannel N , K as the total number of SSs in the system and w denote as the weighting factor, ranging from 0 to 1. The usage factor of subchannel N during the current iteration, say t , is defined as follows

$$U_{N(t)} = U_{N(t-1)} \times w + \frac{U_{N(t-1)} \times (1-w)}{\frac{C_N}{(K-1)} + 1}. \quad (1)$$

When a subchannel is selected and allocated to more than one SS, the usage factor of that subchannel would be reduced by Eq. (1) accordingly. Contrarily, the usage factor of a subchannel that is not selected by any SS remains unchanged. However, as a consequence of subsequent normalization process, unselected subchannels will increase their usage factors whereas those selected subchannels will decrease their usage factors. In the result, the usage factor of unselected subchannel will be much close with the usage factor of selected subchannel. Furthermore, some of the SSs which select the same subchannel may choose another subchannel to transmit because the usage factor of original selected subchannel may become smaller than another usage factor of unselected subchannel. The above process is repeated until each subchannel is only allocated to one SS. After a number of iterations, the subchannels are allocated by random fashion or some forceful criteria in the case that there is still any subchannel selected by more than one SS. At most of times, the subchannel allocations are not the optimal results.

In paper [2], the paper proposed an amended method to improve the performance of the method proposed in paper [1]. The amended method divides all subcarriers into a larger number of subchannels and allocates one or more subchannels to each SS. As a result, the system performance is improved if the number of subchannels allocated to SS, which has the better channel condition, is increased. The arising probability of avoiding deep channel fading is resulted from the reduction of the number of subcarriers in each subchannel. However, the drawback of the proposed method is that the number of subchannels for an SS must be given first before the scheduling.

3.2 Hungarian Algorithm (HA)

The Hungarian Algorithm [3] is a famous algorithm to solve ‘minimum’ assignment problem with m workers and m jobs, and there is some limitation and pre-work before using Hungarian algorithm. The Hungarian algorithm needs to form the job assignment matrix, in which each row represents one worker, each column represents one job, and each indicates the cost if the job is assigned to the related worker. First, if the number of workers does not equal to the number of jobs, one should add dummy workers or jobs with zero costs as needed to make the matrix become m by m matrix. The optimal job assignment is the assignment with the minimal cost summation of all jobs assigned to workers, one for each. The steps of Hungarian algorithm are listed as follows:

- Step 1 : For each row, subtract the minimum number in that row from all numbers in that row.
- Step 2 : For each column, subtract the minimum number in that column from all numbers in that column.
- Step 3 : Draw the minimum number of lines to cover all zeroes. If this number = m , then STOP. An assignment can be made now.
- Step 4 : Subtract d (the minimum uncovered number) from uncovered numbers. Add d to numbers covered by two lines. Numbers covered by one line remain the same. Then, go to Step 3.

Then, find the minimum number of lines and determine the optimal solution.

- Step 1 : Find a row or column with only one unlined zero and circle it. (If all rows/columns have two or more unlined zeroes choose an arbitrary zero.)
- Step 2 : If the circle is in a row with one zero, draw a line through its column. If the circle is in a column with one zero, draw a line through its row. One approach, when all rows and columns have two or more zeroes, is to draw a line through one with the most zeroes, breaking ties arbitrarily.
- Step 3 : Repeat Step 2 until all circles are lined. If this minimum number of lines equals m , the circles provide the optimal assignment.

Notably, if we want to solve the ‘maximum’ assignment problem, we need transform a the profit matrix as the needed cost matrix, in which the new cost value of every entry is equal to the absolute value of the result of original profit minus the maximal profit in profit matrix. In a word, the profit matrix is transformed to a cost matrix, and it is suitable to be solved by Hungarian algorithm.

In our system, we divide whole data subcarriers into several subchannels and use the channel information (such as RSSI, SNR, etc.) as the profit value. Considering the profit matrix $H1$ for example, the values in matrix are assumed to be the channel conditions with respect to SSs and a larger value means a better channel condition is. Symbols A , B , C and D denote the four different SSs (rows) in the system, and the whole data subcarriers are divided into four subchannels (columns).

$$H1 = \begin{matrix} A \\ B \\ C \\ D \end{matrix} = \begin{bmatrix} 20 & 43 & 26 & 60 \\ 42 & 84 & 6 & 9 \\ 13 & 75 & 70 & 60 \\ 41 & 69 & 67 & 96 \end{bmatrix}$$

Here, we want to find the subchannel assignment with the maximal profit summation from the profit matrix. As shown in matrix $H2$, we abstract all profit values from the maximal profit first. In the result, the profit matrix is transformed to the cost matrix, and it is standard form for Hungarian algorithm to find the minimal cost solution.

$$H2 = \begin{matrix} A \\ B \\ C \\ D \end{matrix} = \begin{bmatrix} 76 & 53 & 70 & 36 \\ 54 & 12 & 90 & 87 \\ 83 & 21 & 26 & 36 \\ 55 & 27 & 29 & 0 \end{bmatrix}$$

Next, we subtract each profit value by the minimal profit of each row and following by each column. It is shown in matrix $H3$.

$$H3 = \begin{matrix} A \\ B \\ C \\ D \end{matrix} = \begin{bmatrix} 0 & 17 & 29 & 0 \\ 2 & 0 & 73 & 75 \\ 22 & 21 & 0 & 15 \\ 15 & 27 & 24 & 0 \end{bmatrix}$$

As shown in matrix $H3'$, it is fortunate that we can draw four lines to cover all zeros in the matrix.

$$H3' = \begin{bmatrix} A \\ B \\ C \\ D \end{bmatrix} = \begin{bmatrix} 0 & 17 & 29 & 0 \\ 2 & 0 & 73 & 75 \\ 22 & 21 & 0 & 15 \\ 15 & 27 & 24 & 0 \end{bmatrix}$$

Now, we can find the optimized solution from matrix $H3'$ and the subchannel assignment is shown as matrix $H4$, in which the maximal profit will be achieved if we assign the first subchannel to the SS A, the second subchannel to SS B, the third subchannel to SS C and the fourth subchannel to SS D. With this assignment, the total profit is $20+70+84+96=270$. It is indeed an optimal solution to this problem, and paper [3] has proved that the Hungarian algorithm can always find the best assignment.

$$H4 = \begin{bmatrix} A \\ B \\ C \\ D \end{bmatrix} = \begin{bmatrix} \textcircled{1} & 0 & 0 & 1 \\ 0 & \textcircled{1} & 0 & 0 \\ 0 & 0 & \textcircled{1} & 0 \\ 0 & 0 & 0 & \textcircled{1} \end{bmatrix} \tag{6}$$

3.3 Enhanced Dynamic Frequency Allocation Algorithm

Although we can get the optimal channel information by using Hungarian Algorithm, each SS just can be allocated to the pre-determined number of subchannels. In fact, while one SS suffers from bad channel condition, the SS still can get the pre-determined number of subchannels. If these subchannels can be dynamically allocated to the other SSs with better channel condition, the system throughput might be increased. To meet the goal, we modify the original Hungarian Algorithm to solve the flexible subchannel assignment problem.

Here, we define a metric used for determining the maximal number of subchannels which can be allocated to each SS. The metric is defined as follows:

$$C = \frac{P}{N} \times n \tag{7}$$

where P is the number of subchannels, N is the number of SSs, and n is the enlarging factor for providing the chance for proper SS(s) to get more subchannels. The parameter n varies from 1 to infinity and it is used to control the maximal number of subchannels which can be allocated to one SS, and P/N means the average number of subchannels per SSs in this system. So, the profit matrix is extended by duplicating the channel information as needed. The problem now becomes that we have P subchannels that are to be allocated to $C \times N$ SSs. For example, we divide the whole data subcarriers into four subchannels ($P=4$) and there are four SSs ($N=4$) in this system. When $n=2$, we have $C=2$. The profit matrix, say $H5$, is extended to $C \times N$ by $C \times N$ matrix, in which the channel information values in entries of dummy columns are filled with 0. Notably, it is possible that some SS get no subchannel to transmit, but no SS will use all subchannels alone.

$$H5 = \begin{matrix} A_1 \\ A_2 \\ B_1 \\ B_2 \\ C_1 \\ C_2 \\ D_1 \\ D_2 \end{matrix} = \begin{bmatrix} 76 & 53 & 70 & 36 & 0 & 0 & 0 & 0 \\ 76 & 53 & 70 & 36 & 0 & 0 & 0 & 0 \\ 54 & 12 & 90 & 87 & 0 & 0 & 0 & 0 \\ 54 & 12 & 90 & 87 & 0 & 0 & 0 & 0 \\ 83 & 21 & 26 & 36 & 0 & 0 & 0 & 0 \\ 83 & 21 & 26 & 36 & 0 & 0 & 0 & 0 \\ 55 & 27 & 29 & 0 & 0 & 0 & 0 & 0 \\ 55 & 27 & 29 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

After transforming the general problem to standard form, we can use Hungarian algorithm to get the matrix *H6*. The maximal channel gain will be achieved if we assign the first subchannel to B1, the second subchannel to B2, the third subchannel to C1 and the fourth subchannel to D1. With the assignment the total profit becomes 42+84+70+96=292, and it is better than the total profit 272 derived by using original Hungarian algorithm (see matrix *H4*). Notably, with this assignment, SS A does not get any subchannel, SS B gets two subchannels and SSs C and D both get one subchannel. In summary, if some SS suffers from bad channel condition, it may not be assigned any subchannel. On the other hand, SS with better channel condition might get more subchannels to transmit data frames.

$$H6 = \begin{matrix} A_1 \\ A_2 \\ B_1 \\ B_2 \\ C_1 \\ C_2 \\ D_1 \\ D_2 \end{matrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

4 Simulation Model and Results

Similar to paper [1], we evaluate the effectiveness of the proposed method in the frequency selective Rayleigh channel with AWGN using Monte Carlo simulation method. We assumed that it is a four-user OFDMA system with 64 subcarriers, and these subcarriers are divided into 4 subchannels. In addition, there is no coding schemes or power control methods in the system in order to purely test the effectiveness of the proposed algorithm.

Figure 2 shows the probability of successful allocations of conventional algorithm with iteration method [1], marked as ‘Iteration Algorithm’, and the enhanced dynamic frequency allocation algorithm, marked as ‘Hungary Algorithm’. With iteration algorithm it is possible that the subchannels can’t be totally allocated to users when the number of subchannels increases. Here, we compare the probability of successful allocations between the three algorithms under different numbers of subchannels, varying from 2 to 16. It is obvious that the probability of successful allocations is always 100% by using Hungarian algorithm. Oppositely, the probability of successful

allocations derived from the iteration algorithm decreases as the number of subchannels increases. In the result, with Hungarian algorithm the subcarriers can be divided into more subchannels than iteration algorithms and static algorithm.

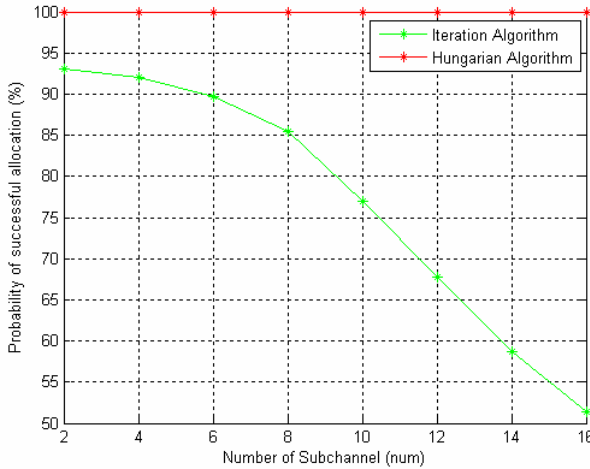


Fig. 2. The probabilities of successful allocations derived from iteration algorithm and Hungary algorithm

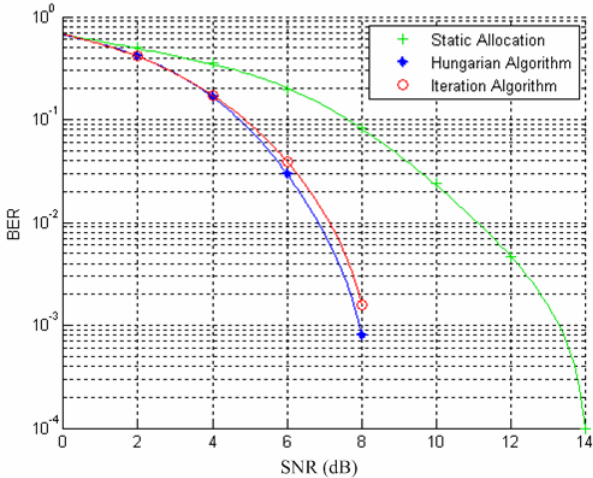


Fig. 3. Bit-Error-Rate comparisons of dynamic and static subcarrier allocation under different SNRs

The performance of subchannel allocation algorithm is the most important thing that is concerned. Figure 3 shows the performance comparisons of BERs derived from static algorithm, iteration algorithm and Hungary algorithm. From the figure, the conventionally static allocation method obtains the worst performance, and the

performance difference among three methods becomes obvious when SNR >4 dB. Furthermore, not only the probability of successful allocation but also the performance with Hungarian algorithm is better than that with iteration algorithm.

Figure 4 shows the capacities of the system with static, iteration and Hungarian subchannel allocation algorithm. It can be seen that as the SNR is considered from 0 to 40 dB, Hungarian algorithm outperforms static and iteration algorithm higher capacity under the same SNR situation. Especially, while the SNR is low the capacity of Hungarian algorithm is twice as much as the capacity of static algorithm.

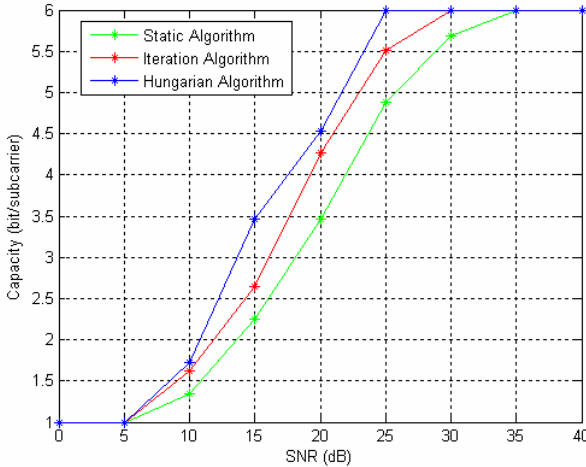


Fig. 4. Performance comparisons of dynamic and static subcarrier allocations in terms of capacity (bit/subcarrier)

5 Conclusion

In this paper, we proposed to use Hungarian algorithm to solve the frequency allocation problem in OFDMA system. The Hungarian algorithm is very suitable to find the optimal allocation in a short response time. However, its restriction is the number of subchannels for an SS must be given before applying Hungarian algorithm. To solve this shortcoming, an enhanced version of Hungarian algorithm is proposed to allow an SS with a better channel condition to use more subchannels than the others. Simulation results show the system throughput and BER are significantly improved by proposed methods.

References

- [1] Choon, T., Alen, H., Madhukumar, A.S., Chin, F.: Capacity enhancement of a multi-user OFDM system using dynamic frequency allocation. *IEEE Trans. Broadcast* 49, 344–353 (2003)
- [2] Chen, Y., Shon, S., Yoo, S.-J., Kim, J.M.: Dynamic frequency selection in OFDMA. In: *ICACT 2006* (February 20–22, 2006)

- [3] Kuhn, H.K.: The Hungarian method for the assignment problem. *Naval Research Logistics Quarterly* 2, 83–97 (1955)
- [4] Chong, E.K.P., Zak, S.H.: *An introduction to optimization*, 2nd edn. John Wiley and Sons, Inc., New York (2001)
- [5] Peng, Y., Doufexi, A., Armour, S., McGeehan, J.: An investigation of Dynamic sub-carrier allocation in OFDMA systems
- [6] Issariyakul, T., Hossain, E.: Optimal Radio Channel Allocation for Fair Queuing in Wireless Data Networks. *Parallel and Distributed Systems*, *IEEE Transactions* 13(11), 1124–1138 (2002)
- [7] Zhang, Z., He, Y., Chong, E.K.P.: Opportunistic downlink scheduling for multiuser OFDM systems. In: *Wireless Communications and Networking Conference 2005*, vol. 2, pp. 1206–1212. IEEE, Los Alamitos (2005)
- [8] van Nee, R., Prasad, R.: *OFDM for wireless multimedia communications*. Artech House Publisher, Boston, London (2000)

Wireless Network Management System for WiMAX / Wi-Fi Mesh Networks

Li-Der Chou, Shih-Yao Cheng, Chien-Yi Li, and Shing-Kuang Chen

Department of Computer Science and Information Engineering,
National Central University
No. 300, Zhongda Rd., Zhongli City, Taoyuan County 32001, Taiwan, R.O.C.
cld@csie.ncu.edu.tw

Abstract. The development of integrating several wireless network technology make wireless network devices built everywhere. In 1999, IEEE proposes WiMAX broadband wireless technology which has high transmission bandwidth and wide coverage. There are more and more researches as above-mentioned wireless technology to increase Mesh network technology which can easily increase network coverage. Intel[1] point out that integrated WiMAX/Wi-Fi Mesh network is the best solution currently. The SS of WiMAX will the bottleneck of network traffic in WiMAX/ Wi-Fi Mesh hierarchy architecture, thus we need to manage the bandwidth between WiMAX and Wi-Fi, and support Mesh network topology development.

Keywords: WiMAX, Wi-Fi, Mesh, Wireless Network, Network Management, bandwidth allocation.

1 Introduction

With the rapid development of wireless[2] network technologies, people look forward to experience the omnipresent internet service[3].

There are also various projects which use different technologies to build up wireless metropolitan area networks worldwide, WMAN for short. . IEEE 802.16 Working Group on Broadband Wireless Access develops WMAN that can provide high bandwidth of 70Mbps and long distance of 40km for wireless access. According to the properties we mentioned above, WiMAX could be the solution of last-mile of home user or small and medium enterprise.

IEEE 802.16's Network Management Task Group which has been set up at 2004 aims to institute management protocol of 802.16 wireless network. IEEE 802.16f-2005 standard has been released at 2005 to set 802.16-2004 the MAC layer and PHY layer of fixed broadband wireless access devices and management information base (MIB), and provide 802.16 how to setup the standard of managed object. Project 802.16g draft define manager process and service, and for IEEE802.16-2004 and IEEE802.16e across fixed and mobile devices, set up standard of network management at mutual network management. Project802.16i define 802.16e MAC layer and PHY layer's MIBs of mobile broadband wireless access device.

In WMNs deployment, each mesh node not only provides wireless service to users, but transferring packet on behalf of other nodes. Wi-Fi is already matured, and WiMAX is developing gradually. Both of them established Task groups (TGs) to specify new standard for mesh networking, such as 802.11s [4] and 802.16j [5].

Two important management functions are needed to maintain the appropriate operation of such integrated networks. The radio management used to maintain appropriate air link status, and the bandwidth management between WiMAX/ Wi-Fi mesh networks[6] are used to allocate bandwidth to Wi-Fi mesh networks connected with WiMAX network. We develop a WiMAX/ Wi-Fi mesh network management system to provide bandwidth allocation strategy among multiple Wi-Fi mesh networks based on monitoring WiMAX/ Wi-Fi mesh networks and estimating current available bandwidth on WiMAX SS.

The rest of this paper is organized as follows. In section 2, it introduces the background of WiMAX and wireless mesh network. In section 3, it proposed a hierarchical WiMAX/ Wi-Fi mesh NMS and described each module and function. Following in section 4, an implemented system is introduced, and in section 5, it discusses two experiments for measure bandwidth in the real network environment and measure bandwidth with bandwidth allocation and conclusions. The future works are given in section 6.

2 Related Work

In 1999, IEEE 802.16 Working Group on Broadband Wireless Access start to develop standardize WMAN access interface. The development of this new standard not only stand for this technology matured but also bring lower cost of establish and network access anywhere. IEEE 802.16 standard develop going through a series of variations[7], from the begging of standard IEEE 802.16 release at 2002 using 10 - 66GHz high frequency broadband, and line-of-sight transition property, 50 kilo-meter transmission range and 72 million bits per second transmission speed at Point-to-Point mode; to improve the usage of application, IEEE 802.16 working group release 802.16a which using 2-11GHz and none-line-of-sight transmission property, at most 6.5 kilo-meter transmission range at Point-to-Multipoint mode; by a series of modify, IEEE 802.16-2005[8] define fixed broadband wireless access system has been release at 2004, which define two properties smaller then 11GHz line-of-sight transmission system and 10-66GHz none-line-of-sight transmission system. At 2005, IEEE 802.16 release 802.16f which define Management Information. Base for fixed BWA, and define 802.16e draft-standard in order to support mobile devices.

Owing to more and more people pay close attention to this standard, Nokia and many communication companies set up WiMAX forum[9] at 2001 April. The major purpose of WiMAX forum is the orientation of IEEE 802.16, handle the communication between different brand, authentication and deal out frequency spectrum. WiMAX is regarded as one of the most important technology of broad band wireless technologies, such kind of standard is IEEE 802.16-2004 and IEEE 802.16e. Due to IEEE 802.16-2004 support fixed wireless access service, all devices which use 802.16-2004 are usually look upon to WiMAX-fixed. Now, the major development uses the property of none-line-of-sight and point-to-multi-point to would replace the

last-mile gradually and greater than 10GHz to support broad bandwidth. It is suitable for network backhaul's application. And wireless devices using 802.16e usually look upon to WiMAX-mobile, supporting mobile host in WiMAX network can access WiMAX network directly.

3 Design of Wireless Network Management System for WiMAX/ Wi-Fi Mesh Networks

There are two assumptions in the WiMAX/ Wi-Fi mesh NMS. At first, all of the WiMAX/ Wi-Fi mesh devices need SNMP supporting; and the other assumption is that the devices must support ICMP PING or we need to know the IP address of WiMAX BS.

This paper proposed the WiMAX/ Wi-Fi mesh NMS network management architecture as Figure 1; it has two major tasks which are described as follows:

Firstly, the Wi-Fi mesh NMS manages Wi-Fi APs and Wi-Fi mesh APs. The WiMAX mesh NMS not only manages WiMAX BS and SS, but also collects statistic information from Wi-Fi mesh NMS. Secondly, WiMAX/ Wi-Fi mesh NMS update the data of WiMAX/ Wi-Fi mesh devices constantly.

The system analyses from the user point are divided into two parts: one is from the client side and the other is from the server side. The client side only needs JAVA language supporting. And the server side includes the management system that provides all functions and services; the design of server side is divided into six parts as follows: Graphical User Interface (GUI) module, Authentication module, Discovery module, Performance module, Monitor module, Bandwidth module.

The section introduces the functions of each module on WiMAX/ Wi-Fi mesh NMS. It also presents these functionalities and usages that can be achieved through the proposed architecture in each module. All of these functionalities work with devices which must have SNMP agent supporting.

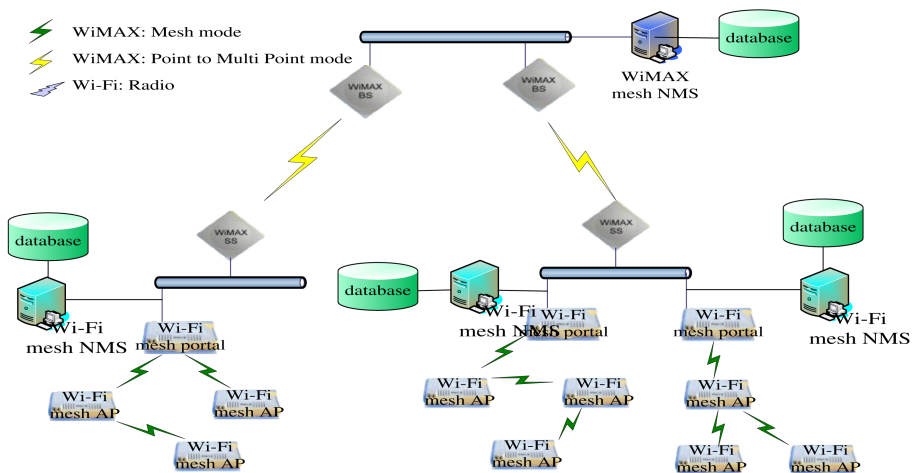


Fig. 1. Architecture of WiMAX/ Wi-Fi mesh network management system

(1) Functions of GUI module

Device topology: this function provides the physical mapping of the discovered devices. It shows as the hierarchical tree architecture. It is convenient for managers to see the relationship of whole network. Discovery request: the manager could input a range of IP address or input an IP address for WiMAX BS, and then the GUI module would send the request to Discovery module. Change modulation type: the managers can change modulation type on WiMAX BS and SS on demand, the WiMAX/ Wi-Fi mesh NMS supports 7 different modulation types such as BPSK 1/2, QPSK 1/2, QPSK 3/4, 16QAM 1/2, 16QAM 3/4, 64QAM 2/3 and 64QAM 3/4. Power selection: the managers can use this function to change the power level of interfaces on Wi-Fi mesh AP individually. The Wi-Fi NMS implements four power levels such as 100%, 50%, 25% and 12.5%. Interface selection: the managers can use this function to select which interface to monitored or controlled.

(2) Functions of authorization module

Authentication manager log: this function provides the history manager logs that manager login time and logout time. Manager action log: this function provides the history manager action logs that records the manager behaviors during the using time.

(3) Functions of discovery module

Wi-Fi AP: this function can discover Wi-Fi devices in the managed domain. Wi-Fi mesh AP: this function can discover Wi-Fi mesh AP in the managed domain. WiMAX BS: this function can discover WiMAX BS in the managed domain, and find out the SSs connected with BS. WiMAX SS: this function can discover WiMAX SS in the managed domain.

Functions of performance module:

Input statistics: the function provides the input traffic report. Output statistics: the function provides the output traffic report. Probability density function: the function provides the p.d.f report. Cumulative distribute function: the function provides the c.d.f report.

(4) Functions of monitor module

WiMAX monitoring: the function provides the ability to monitor WiMAX MIB, which could monitor WiMAX SS directly or via WiMAX BS. Wi-Fi monitoring: the function provides the ability to monitor Wi-Fi MIB. Wi-Fi mesh monitoring: the function provides the ability to monitor a Wi-Fi mesh networks in hierarchical way.

(5) Functions of bandwidth module:

Estimated bandwidth[10][11]: the function could estimate current bandwidth on WiMAX SS while SS changed modulation type. Strategy[12]: the function compiles bandwidth allocation strategy for multiple Wi-Fi mesh networks connected with a WiMAX SS. There are two strategies in the system. The first one is "static" which allocate bandwidth by SS table written by estimated bandwidth function. The other one is "percentage" which allocates bandwidth is according with the need of available and request. Active: the function sends bandwidth allocation strategy to WiMAX SS and actives bandwidth allocation function on SS.

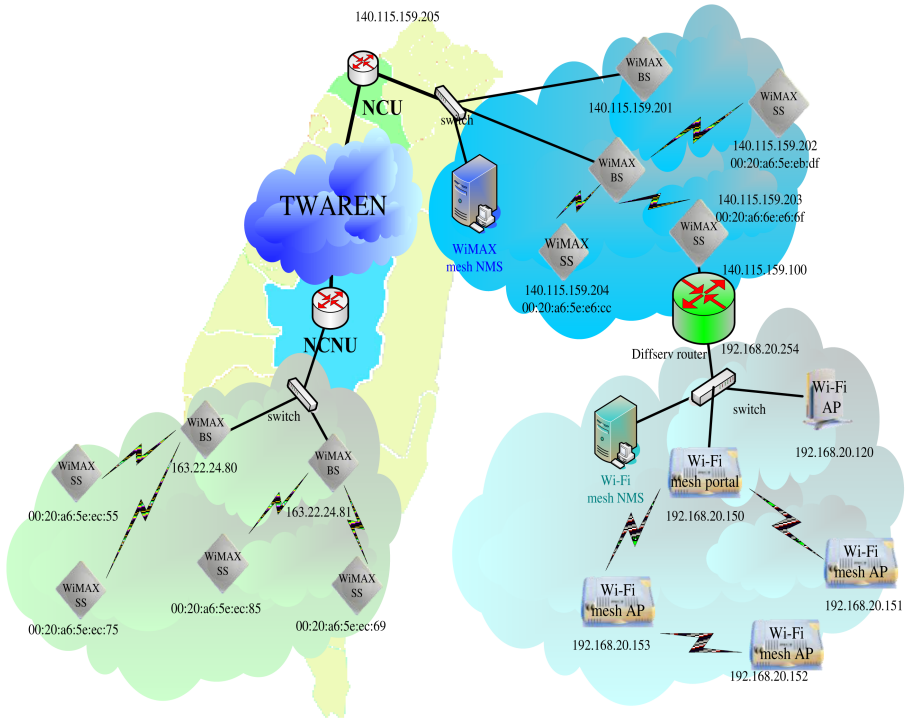


Fig. 2. Implementation environment

4 Implementation Environment and Develop Tools

It becomes more important issue that needs to be solved is how to integrate and manage the different wireless networks which includes WiMAX/ Wi-Fi mesh networks efficiently. In 2005, NCU and NCNU established a WiMAX networks test environment, and we plus a Wi-Fi mesh network connected with the NCU WiMAX SS. Figure 2 shows the deployment environment. In NCU, there are two Proxim MP16 3500[13] BSs installed at the rooftop of the Library, each equipped a 60° antenna. The Proxim MP16 3500 SSs are installed at the rooftop of the electrical engineering building, communication center and lefting one for portable test. In NCNU, there are also two Proxim MP16 3500 BSs and four Proxim MP16 3500 SSs be installed in the campus. We implement the WiMAX/ Wi-Fi mesh NMS for the networks which could be divided into two parts: At first, WiMAX mesh NMS is set in the library of the NCU which are used to manage WiMAX networks in NCU and NCNU, and the Wi-Fi mesh NMS is setting in the lab which are used to manage the private Wi-Fi mesh networks.

We use the Windows XP SP2 as the development and implementation platform. The develop environment that we need is to install JDK 1.5.0 which makes JAVA program executable, then we install Apache as the WEB server which is the most popular WEB server currently and Tomcat for execute JSP program, and MySQL as database server. Table 1 show several tools utilized during the developing process.

We use the JAVA language to build the kernel of most modules and Java Server Pages (JSP), JAVA Script and JAVA Applet to build a familiar GUI for managers. All of them can be executed in all kinds of operation systems and all develop tools are open source. It also uses the free application programming interface (API) of Westhawk's Java SNMP stack 4_13 to implement SNMP operation for requesting the data set of WiMAX/ Wi-Fi mesh devices, and use MG-SOFT Browser to verify the SNMP operation be executed correctly in the proposed system.

The implementation of the proposed system could be divided into two parts, such as WiMAX mesh NMS and Wi-Fi mesh NMS. WiMAX mesh NMS could management the WiMAX mesh devices and get information from Wi-Fi mesh devices by connecting to Wi-Fi mesh NMS. We have a web-based GUI used to communicate with manager, who log into the system by verifying name and password. After verifying, the system shows main page on web browser, and it be divided into three frames. At first, the top frame could discover the WiMAX devices on WiMAX mesh NMS by input a range of IP addresses or adding IP address for known WiMAX BS, and discover the Wi-Fi mesh devices on Wi-Fi mesh NMS, then monitor the module would find out the WiMAX SSs connected with the BS automatically. Secondly, the right frame shows the topology of the WiMAX/ Wi-Fi mesh network on the WiMAX mesh NMS. Finally the left frame shows the discovery result, list of the managed devices and the advanced information for configuring WiMAX/ Wi-Fi mesh devices, the function of power selection are implemented with interfaces on Wi-Fi mesh AP and the function of change modulation type are implemented on WiMAX devices.

5 Experiments and Discussions

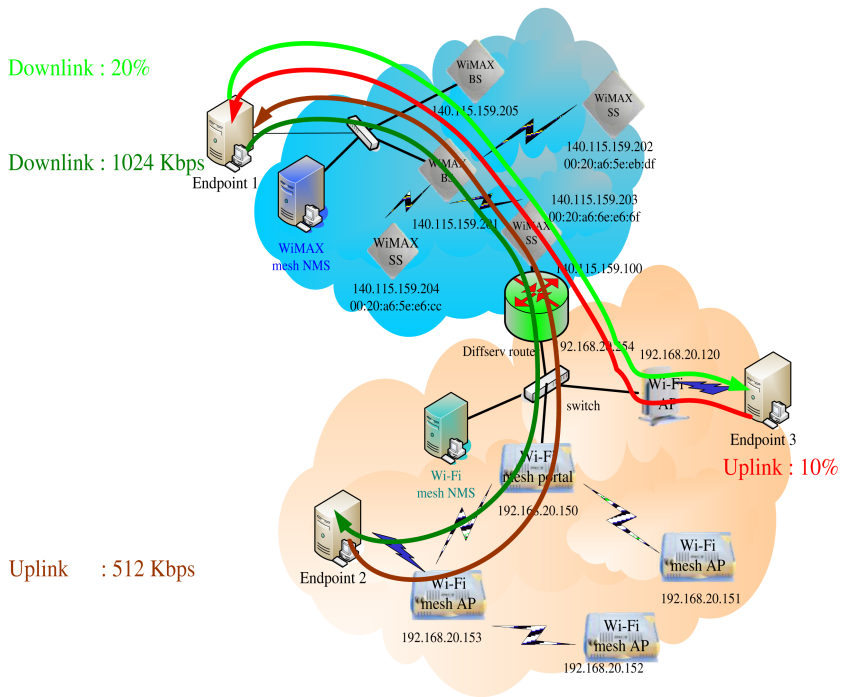
Experiment results and discussions are presented in this chapter. The experimental environment as shown in Figure 3, the experiment adopts "static" bandwidth allocation strategy for endpoint 2 for uplink takes 512 Kbps of estimated bandwidth and downlink takes 1024 kbps of estimated bandwidth and adopts "percentage" bandwidth allocation strategy for endpoint 3 for uplink takes 10% of estimated bandwidth and downlink takes 20% of estimated bandwidth. The traffic generator generates traffic between endpoint 1 and endpoint 2, endpoint 3, and record the result for discussion. We changed modulation types for testing if the system could allocate bandwidth to different Wi-Fi mesh networks connect with the same WiMAX SS according to the bandwidth allocation strategy for each Wi-Fi mesh network.

Table 1. Develop tools

| Develop tools | Name and Version |
|----------------------|---|
| Language | JAVA, JSP 2.0, JAVA Script |
| Programming Platform | Eclipse V.3.0.1 Macromedia Dreamwaver MX |
| SNMP agent | Westhawk's Java SNMP stack 4_13 |
| MIB browser | MG-SOFT Browser Edition 7.10.0.3880 |

Table 2. Result of experiment 1

| Modulation | Mean bandwidth in uplink | Mean bandwidth in downlink | Standard deviation in uplink | Standard deviation in downlink |
|------------|--------------------------|----------------------------|------------------------------|--------------------------------|
| 64QAM3/4 | 500 | 1149 | 0.05779 | 0.131916 |
| 42QAM2/3 | 426 | 834 | 0.03167 | 0.09671 |
| 16QAM3/4 | 505 | 1138 | 0.04977 | 0.15817 |
| 16QAM1/2 | 505 | 1070 | 0.06193 | 0.15908 |
| QPSK3/4 | 522 | 876 | 0.03873 | 0.21234 |
| QPSK1/2 | 505 | 633 | 0.06757 | 0.19479 |
| BPSK1/2 | 391 | 352 | 0.04452 | 0.03355 |

**Fig. 3.** Experimental environment

Objective: This experiment compares with “static” and “percentage” bandwidth allocation strategies for Wi-Fi mesh networks connected with WiMAX SS. With the monitor of WiMAX SS, the WiMAX/ Wi-Fi mesh NMS detected the modulation change and use associated bandwidth allocation strategies to reallocate bandwidth for multiple Wi-Fi mesh networks. **Method:** All of the endpoints execute endpoint program, then start throughput test in BPSK 1/2, QPSK 1/2, QPSK 3/4, 16QAM 1/2, 16QAM 3/4, 64QAM 2/3 and 64QAM 3/4 modulation for uplink and downlink

direction. Experiments results and discussions: The experiment1 throughputs for Endpoint 2, which be guaranteed static downlink 1024 Kbps and uplink 512 Kbps.

Table 3. Result of experiment 2

| Modulation | Mean bandwidth in uplink | Mean bandwidth in downlink | Standard deviation in uplink | Standard deviation in downlink |
|------------|--------------------------|----------------------------|------------------------------|--------------------------------|
| 64QAM3/4 | 562 | 1211 | 0.04067 | 0.11603 |
| 42QAM2/3 | 484 | 1088 | 0.03167 | 0.09135 |
| 16QAM3/4 | 491 | 843 | 0.03562 | 0.05891 |
| 16QAM1/2 | 243 | 547 | 0.01683 | 0.06280 |
| QPSK3/4 | 184 | 412 | 0.01639 | 0.05504 |
| QPSK1/2 | 125 | 273 | 0.0086 | 0.03753 |
| BPSK1/2 | 57 | 128 | 0.00673 | 0.02304 |

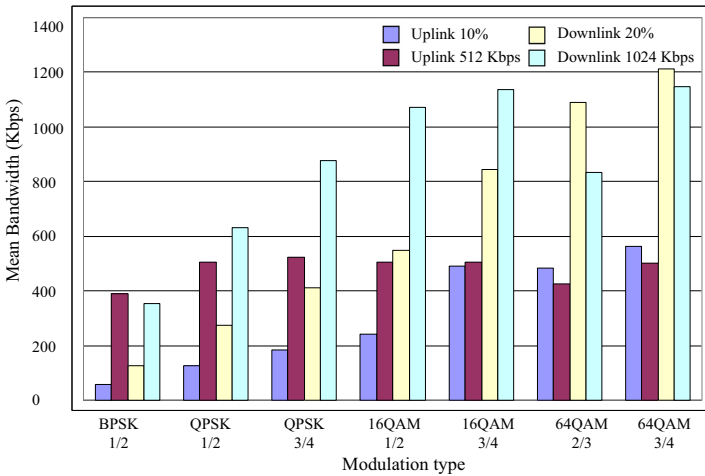


Fig. 4. Mean bandwidth for uplink and downlink with percentage BW allocation strategy in different modulation type

The same situation in experiment2 occurs on uplink while the modulation is less complex than QPSK 1/2. The total bandwidth could not provide enough bandwidth to guarantee the bandwidth agreement. Then the experiment use “percentage” bandwidth allocation policy which is guaranteed 20% of estimated downlink bandwidth and 10% of estimated uplink bandwidth, the experiment proceeded between Endpoint1 and Endpoint3.

We discuss the static and percentage bandwidth allocation strategy in Figure 4, the Wi-Fi mesh network takes less bandwidth by percentage bandwidth allocation strategy when the modulation type less complex than 16QAM 3/4, from the result, the static bandwidth allocation strategy almost allocate much bandwidth to a Wi-Fi mesh

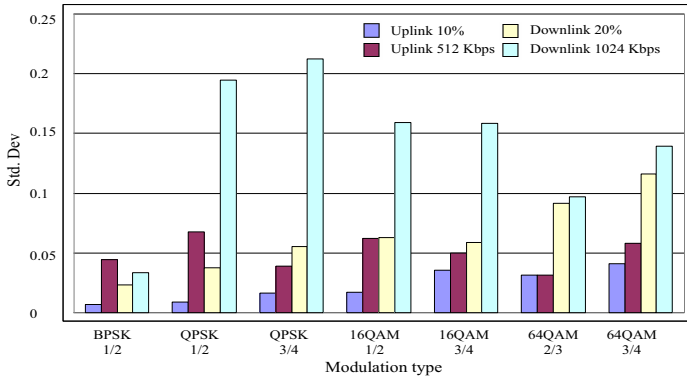


Fig. 5. Standard deviation for uplink and downlink with percentage BW allocation strategy with different modulation type

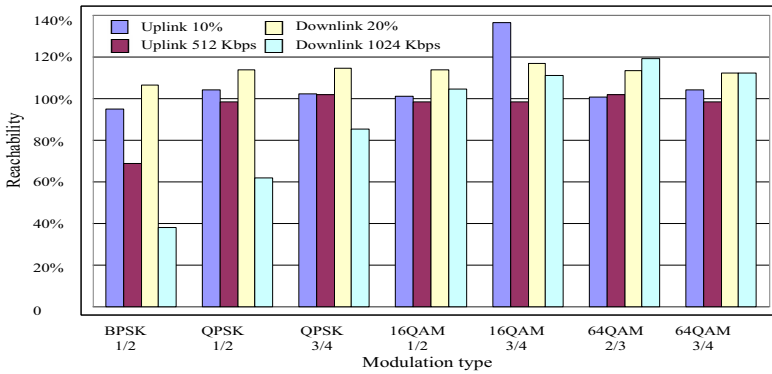


Fig. 6. Reachability for percentage and static bandwidth allocation strategies

networks, however, in Figure 5 shows that it has large standard deviation, which affects the stable service such as VoIP, the percentage allocation policy seems work well in each modulation type, but the guaranteed bandwidth variation large based on modulation type changed, we make a series of experiments with different modulation types for verification. After all, we compares the reach rate for static bandwidth allocation strategy and percentage bandwidth allocation strategy with their expected value, as Figure 6 shows, the reach rate might more than 100%, that is caused by bandwidth management capability of CBQ. In percentage bandwidth allocation strategy, it always keeps reach rate up than 95%, but in static bandwidth allocation strategy, the range of reach rate varies from 38% to 119%, even the Wi-Fi mesh NMS get the information of SS, it could not estimated the bandwidth he would get correctly. Considering of this situation, the percentage bandwidth allocation strategy works better.

6 Conclusions

In this paper, first of all we explain the importance of WiMAX/ Wi-Fi mesh network management system in the WiMAX/ Wi-Fi mesh networks, and introduce the architecture of our proposed WiMAX/ Wi-Fi mesh network management system. Monitor module and bandwidth module, which could monitor the WiMAX/ Wi-Fi mesh network status and reallocate bandwidth to multiple Wi-Fi mesh networks connected with a WiMAX SS accordingly. We provide “static” and “percentage” bandwidth allocation schemes, in static way, the mesh network are always promised a static bandwidth, it is more less complexity than percentage way, the “percentage” bandwidth allocation scheme provides high flexibility but increase system load by reallocating in each modulation type changed, the two kinds of bandwidth allocation schemes could be apply for different service need.

Acknowledgments

This research was supported in part by National Science Council of the Republic of China under contracts NSC 93-2219-E-260-006, NSC 95-2627-E-008-002 and NSC 95-2221-E-008-031.

References

1. Intel Corp., Understanding Wi-Fi and WiMAX as Metro-Access Solution (2004), <http://www.intel.com/netcomms/technologies/wimax/304471.pdf>
2. Chou, L.-D., Lu, C.-C., Lu, C.-Y.: Design of location management for heterogeneous wireless networks. LNCS. Springer, Heidelberg (to appear, 2007)
3. Chou, L.-D., Chen, J.-M., Kao, H.-S., Wu, S.-F., Lai, W.: Seamless streaming media for heterogeneous mobile networks. ACM Springer Mobile Networks and Applications 11(6), 873–887 (2006)
4. Hauser, J.: Draft PAR for IEEE 802.11 ESS Mesh, IEEE Document Number: IEEE 802.11-03/759r2
5. IEEE 802.16's Mobile Multihop Relay (MMR) Study Group, <http://ieee802.org/16/sg/mmr/>
6. Chou, L.-D., Hsieh, H.-J., Chen, J.-M.: Multicast with QoS support in heterogeneous wireless networks. In: Yang, L.T., Guo, M., Gao, G.R., Jha, N.K. (eds.) EUC 2004. LNCS, vol. 3207, pp. 581–590. Springer, Heidelberg (2004)
7. Eklund, C., Marks, R.B., Standwood, K.L., Wang, S.: IEEE Standard 802.16: A Technical Overview of the WirelessManTM Air Interface for Broadband Wireless Access. IEEE Communications Magazine, pp. 98–107 (June 2002)
8. Marks, R.B., Stanwood, K., Chang, D.n.: IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Standard (October 2004)
9. WiMAX Forum, <http://www.wimaxforum.org>

10. Chen, Y.W.: Traffic Behavior Analysis and Modeling of Sub-networks. *International Journal of Network Management* 12(5), 323–330 (2002)
11. Chen, Y.W., Chou, C.-C.: Correlation based Traffic Modeling of Sub-networks. *Journal of Internet Technology*
12. Chen, Y.W., Hu, S.-H.: Study of the Traffic Scheduler by Using Correlation Heuristics. *IEICE Trans. on Communications*, 2273–2280 (2004)
13. Proxim Wireless Achieves WiMAX Forum Certification for Tsunami® MP.16 3500 Product, http://www.proxim.com/products/bwa/multipoint/16_3500/index.html

An Implementation of QoS Framework for Heterogeneous Networks

Chang-Yang Ho and Hsi-Lu Chao

Department of Computer Science
National Chiao Tung University
hlchao@cs.nctu.edu.tw

Abstract. Due to the popularity of the IEEE 802.11-based LANs and fast development of the IEEE 802.16e MANs, we can expect a heterogeneous network consisting of 802.11-based and 802.16e networks in the near future. In such an environment, heterogeneous handoff is possible. How to keep guaranteeing the handoff connection its QoS demand, and in the meantime, avoid impacting on other connections is a challenge to support real-time applications in a heterogeneous network. In this paper, we develop a heterogeneous network in NS-2 simulator. In addition, we implement application mapping function, call admission control, and scheduling in this heterogeneous network to observe the QoS performance of a handoff connection. The simulation results show that our implemented modules support handoff connections' QoS demands in respect of throughput, and delay. In addition, the implemented call admission control algorithm reduces the blocking rate efficiently.

Index Terms: Call admission control, scheduling, heterogeneous network, heterogeneous handoff.

1 Introduction

The IEEE 802.11-b/a/g is the most popular medium access control (MAC) protocols and physical (PHY) schemes in recent wireless communication. However, it does not support quality of service (QoS), which is essential in real-time multimedia applications. Therefore, IEEE 802.11e [1] was proposed and it is a supplementary standard of 802.11 to provide priority-based service differentiation for different kinds of applications. All applications are classified into four access categories (ACs): AC_VO (voice), AC_VI (video), AC_BE (best effort), and AC_BK (background). The service differentiations among four ACs are achieved by assigning each AC with different Arbitration InterFrame Space (*AIFS*), minimum contention window value (CW_{min}) and maximum contention window value (CW_{max}). The higher priority AC (e.g., AC_VO) has the smaller *AIFS*, CW_{min} , CW_{max} values than those of the lower priority ACs (e.g., AC_VI, AC_BE, and AC_BK).

Due to the recent explosive Internet growth and customers' demands for advanced multimedia services, the IEEE 802.16e [2] is the focus of technology development. Advantages of the IEEE 802.16e system include rapid deployment, high speed data rate, high scalability, multimedia services, and lower maintenance, and upgrade costs. To support services with variable QoS demands, five service classes (SCs) are defined in the IEEE 802.16e system: unsolicited grant service (UGS), real-time polling service (rtPS), enhanced real-time polling service (ertPS), non-real time polling service (nrtPS), and best effort service (BE). QoS parameters a connection can set include minimum reserved rate, maximum sustained rate, maximum latency, and tolerated jitter.

The IEEE 802.16e is designed for metropolitan area networks (MANs), and it has no intention to replace IEEE 802.11e networks. Therefore, we can expect a heterogeneous network consisting of IEEE 802.11e LANs and 802.16e MANs in the near future. When a mobile station (MS) has both IEEE 802.11e and IEEE 802.16e network interface cards, heterogeneous handoff is possible. Here the heterogeneous handoff means that a MS moves from an IEEE 802.11e (or IEEE 802.16e) network to an IEEE 802.16e (or IEEE 802.11e) network. Our motivation is to observe the QoS performance when heterogeneous handoff occurs. The contribution of this paper is the IEEE 802.11e+IEEE 802.16e heterogeneous network development in NS-2 simulator [3]. In addition, we implement several QoS-related modules which are essential for this observation.

The remainder of this paper is organized as follows. Section 2 describes modules and algorithms we implement in NS-2 simulator. Section 3 is the performance evaluation. This paper concludes with Section 4.

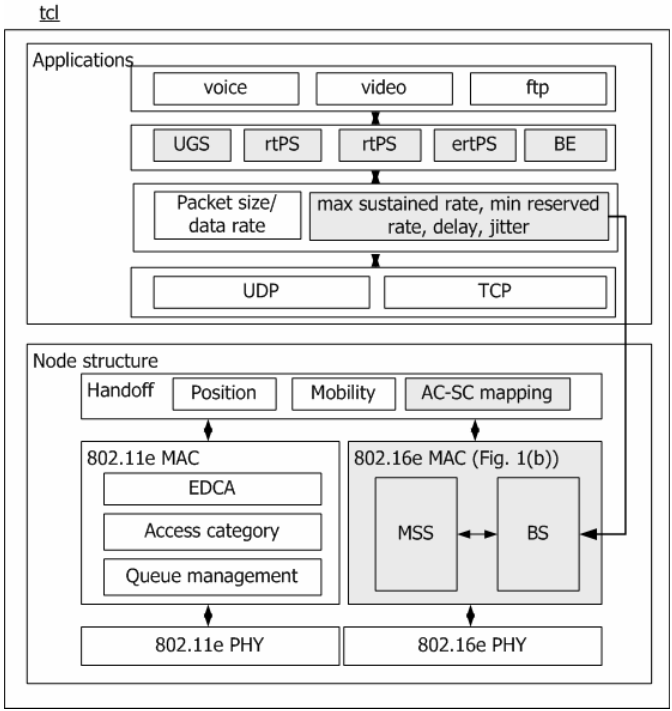
2 The Implemented Modules in NS-2 Simulator

To develop a heterogeneous network and do observation about connections' QoS performance, we implement several modules in the NS-2 simulator. These modules are node configuration, AC-SC mapping, CAC in 802.16e, and scheduling, as shown in Figs. 1(a) and 1(b). In Fig. 1, the existing modules/functions are represented as white blocks, and our implemented/modified modules are shown in gray blocks. We introduce each module in the following.

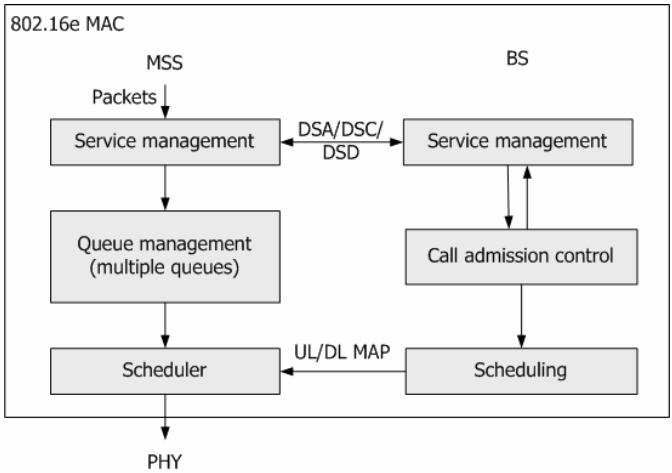
2.1 Access Category-Service Class (AC-SC) Mapping

The function of AC-SC mapping is to transform a connection's AC in IEEE 802.11e (or SC in IEEE 802.16e) to SC in IEEE 802.16e (or AC in IEEE 802.11e) when handoff occurs. The mapping rules are:

- (1) When moving from an IEEE 802.11e-based network to an IEEE 802.16e-based network,
 - (a) the SC of a handoff voice-type connection is set to be UGS;
 - (b) the SC of a handoff video-type connection is set to be rtPS;
 - (c) the SC of a handoff best effort-type connection is set to be either nrtPS or BE;
 - (d) the SC of a handoff background-type connection is set to be BE.



(a) QoS-related modules in NS-2 simulator



(b) Implemented modules in IEEE 802.16e MAC

Fig. 1. Implemented QoS-related modules in the NS-2 simulator

- (2) When moving from an IEEE 802.16e-based network to an IEEE 802.11e-based network,
- the AC of a handoff UGS connection is set to be AC_VO;
 - the AC of a handoff rtPS or ertPS connection is set to be AC_VI;
 - the AC of a handoff nrtPS connection is set to be AC_BE;
 - the AC of a handoff BE connection is set to be AC_BE or AC_BK.

Note that an AC_BE connection could be mapped to nrtPS or BE service class. In the case that an AC_BE connection is accompanied a minimum QoS requirement, then it is mapped to nrtPS service class; otherwise, it is mapped to BE service class. Similarly, connections of BE service class could be mapped to AC_BE or AC_BK and it is determined by whether the QoS requirement is set or not.

When a connection incurs handoff from an IEEE 802.11e network to an IEEE 802.16e network, it first sends a dynamic service addition-request (DSA-REQ) message, which contains its QoS parameter settings, to the BS. The BS executes the AC-SC mapping function, and then does call admission control (CAC). The details of CAC are described in Sec. II.B.

2.2 Call Admission Control (CAC)

In IEEE 802.16e point to multipoint (PMP) mode, when and how long an MSS can send its data packets are determined by the base station (BS). To avoid exceeding the bandwidth and further failing to support QoS, a CAC algorithm is essential for a BS to admit or reject handoff connections' requests. CAC algorithm we implemented is based on the concepts of [4]. Considering a fact that the available channel capacity changes dynamically due to connection handoff, the implemented CAC algorithm has two phases, and both are described in the following.

Phase 1: upon receiving a DSA-REQ message, the BS checks if the handoff connection i 's QoS demand can be satisfied or not. The check is based on the rule listed in (1).

$$rate_{\min}(i) + \sum_{j \in \{UGS\}} rate(j) + \sum_{k \in \{rtPS\}} rate_{\min}(k) + \sum_{l \in \{ertPS\}} rate_{\min}(l) + \sum_{m \in \{nrtPS\}} rate_{\min}(m) \leq \alpha \times C, \quad (1)$$

where $rate_{\min}(i)$ is the minimum QoS demand of the new connection i , and $rate_{\min}(*)$ is the minimum reserved data rate of a connection, and that connection can be rtPS, ertPS or nrtPS service class. C is the channel capacity, α is a predefined constant whose value is within (0, 1] and is used to indicate the percentage of allocated channel capacity. $\{UGS\}$, $\{rtPS\}$, $\{ertPS\}$, and $\{nrtPS\}$ indicate the connection sets of four service classes. Connection i can be admitted entering the IEEE 802.16e network when equation (1) is true.

Phase 2: when the available channel capacity cannot support connection i 's QoS demand and connection i does not belong to $\{UGS\}$, the BS negotiates with the MSS to temporarily lower the requirement by sending dynamic service change-request

(DSC-REQ) message. If the MSS agrees on this suggestion, it then responds a dynamic service change-response (DSC-RSP). The BS then executes scheduling based on the updated QoS demand. The BS records the original minimum QoS requirement for future adjustment, too. In the case that the MSS denies to lower down its requirement, the BS sends the MSS a dynamic service deletion-request (DSD-REQ) to reject its entrance.

The flowchart of CAC algorithm is shown in Fig. 2.

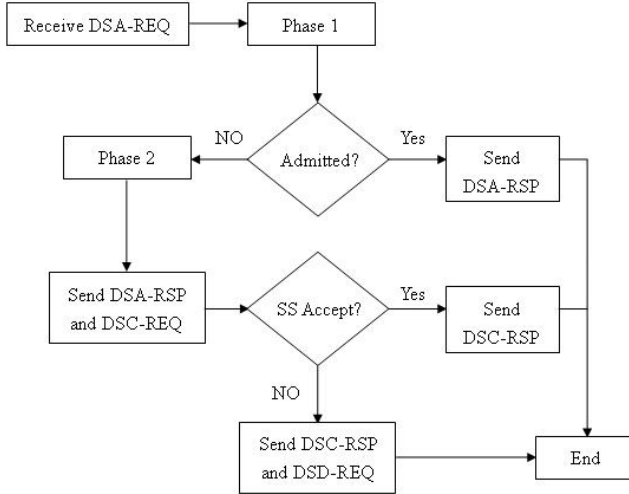


Fig. 2. The flowchart of CAC algorithm

2.3 Scheduling Algorithm

The objective of scheduling algorithm is to allocate bandwidth to all admitted connections to support their QoS demands. To achieve it, we implement two timers in the NS-2 scheduler module. The first timer, denoted as $T_1(i)$ is to satisfy connection i 's minimum requirement (i.e., $rate_{min}(i)$); the second timer, denoted as $T_2(i)$, is used to allocate the could-share residual bandwidth to connection i . Here we assume fixed packet size L in bits. To guarantee connection i with its minimum QoS demand, the connection must transmit at least $rate_{min}(i)/L$ packets per second. That means the BS needs grant connection i one packet transmission opportunity every $L/rate_{min}(i)$ seconds. We set $T_1(i)$ be $L/rate_{min}(i)$. Each time $T_1(i)$ counts down to zero, the BS allocates one packet transmission opportunity to connection i , and then the timer is refreshed to be $L/rate_{min}(i)$ again.

To set $T_2(i)$, we first calculate the residual bandwidth (denoted as $BW_{residual}$) after satisfying all connections' minimum QoS demands, as in (2).

$$\begin{aligned}
 BW_{residual} = & \alpha \times C - \sum_{i \in \{UGS\}} rate(i) - \sum_{i \in \{rtPS\}} rate_{min}(i) \\
 & - \sum_{i \in \{ertPS\}} rate_{min}(i) - \sum_{i \in \{nrtPS\}} rate_{min}(i)
 \end{aligned} \tag{2}$$

We then determine the $BW_{residual}$ share ratio among rtPS, ertPS, nrtPS connection sets, as (3).

$$\begin{aligned} & \sum_{i \in \{rtPS\}} (rate_{max}(i) - rate_{min}(i)) : \sum_{j \in \{ertPS\}} (rate_{max}(j) - rate_{min}(j)) : \\ & \sum_{k \in \{nrtPS\}} (rate_{max}(k) - rate_{min}(k)) = a : b : c \end{aligned} \quad (3)$$

where $rate_{max}(i)$ is the maximum sustained rate of connection i . Thus for connection i, j and k , their could-share residual bandwidth, denoted as $BW_{residual}(i)$, $BW_{residual}(j)$ and $BW_{residual}(k)$ are in (4), (5) and (6).

$$BW_{ex}(i) = \frac{a}{a+b+c} \times BW_{residual} \times \frac{(rate_{max}(i) - rate_{min}(i))}{\sum_{l \in \{rtPS\}} (rate_{max}(l) - rate_{min}(l))} \quad (4)$$

$$BW_{ex}(j) = \frac{b}{a+b+c} \times BW_{residual} \times \frac{(rate_{max}(j) - rate_{min}(j))}{\sum_{l \in \{ertPS\}} (rate_{max}(l) - rate_{min}(l))} \quad (5)$$

$$BW_{ex}(k) = \frac{c}{a+b+c} \times BW_{residual} \times \frac{(rate_{max}(k) - rate_{min}(k))}{\sum_{l \in \{nrtPS\}} (rate_{max}(l) - rate_{min}(l))} \quad (6)$$

Similarly to $T_1(i)$, the BS grants connection i one packet transmission opportunity per $L/BW_{residual}(i)$ seconds. Each time $T_2(i)$ counts down to zero, the BS allocates one packet transmission opportunity to connection i again, and then the timer is refreshed to be $L/BW_{residual}(i)$.

3 Performance Evaluation

In this section, we evaluate the QoS performance when considering handoff in a heterogeneous network by using NS-2 simulator. In NS-2 simulator, we implement several modules including AC/SC mapping, CAC and scheduling.

3.1 Simulation Environments

There are one access point (AP) and 10 motile stations (MSs) in an IEEE 802.11e network; one BS and 15 mobile subscribe stations (MSSs) in an IEEE 802.16e network. The heterogeneous topology is shown in Fig. 3. The bandwidth of IEEE 802.11e and 802.16e networks are 6 Mbps and 20 Mbps, respectively. In our simulation, α is set to be 0.9. The parameter settings of connections in IEEE 802.11e and 802.16e networks are listed in Table 1. We do not simulate best effort connections in our experiments.

The performance metrics include throughput, delay and blocking rate, and their definitions are described below.

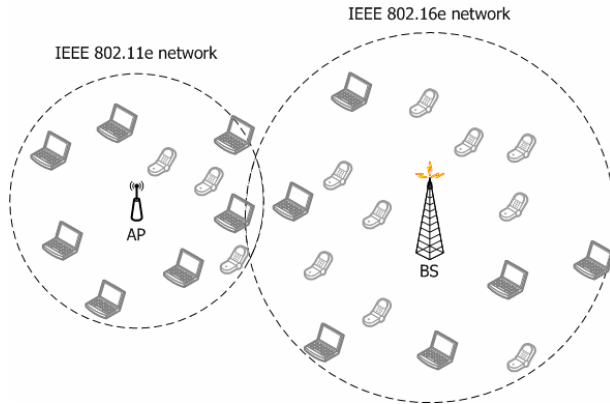


Fig. 3. Network topology in our simulation

Table 1. Connection settings in both IEEE 802.11e and 16e networks

| IEEE 802.11e | | | | IEEE 802.16e | | | | |
|--------------|-------------|------------------|------------|--------------|-----------------|-----------------|------------------|------------|
| Priority | Rate (Kbps) | Pkt size (bytes) | Max. delay | | Max rate (Kbps) | Min rate (Kbps) | Pkt size (bytes) | Max. delay |
| 1 | 56 | 210 | 25 ms | UGS | 56 | 56 | 210 | 25 ms |
| | | | | rtPS | 1024 | 128/256/512 | 512 | 100 ms |
| 2 | 1024 | 512 | 100 ms | ertPS | 1024 | 128/256/512 | 512 | 100 ms |
| | | | | nrtPS | 128/256 | 32 | 512 | 200 ms |
| 3 | 128/256 | 512 | 200 ms | | | | | |

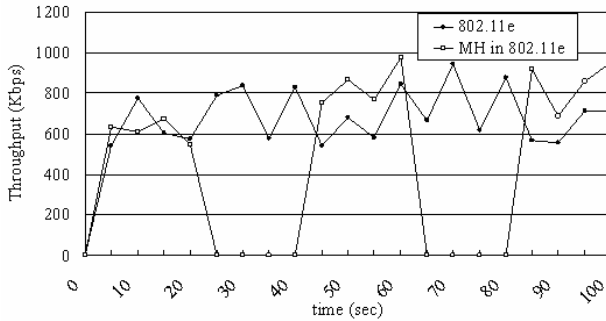
- (1) Throughput (Φ_i): the successfully transmitted data of the specific AC or SC i divided by the simulation time.
- (2) Delay (d_i): the average packet delay time of the specific AC or SC i . we only count the successfully transmitted packets in.
- (3) Blocking rate: the percentage of handoff connections which are rejected by the BS to enter the IEEE 802.16e network due to failed CAC check.

3.2 Simulation Results

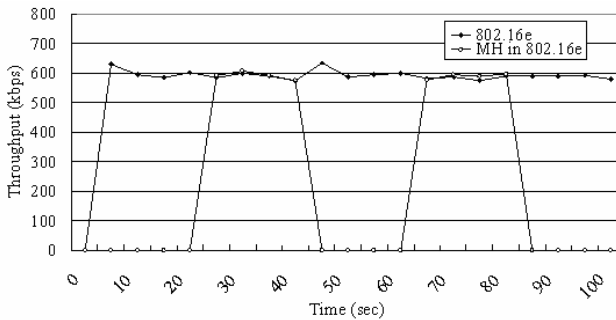
3.2.1 QoS Performance of the Handoff Connection

In this experiment, an MS/MSS handoffs between the IEEE 802.11e and 802.16e networks periodically. We set the period be 20 seconds, that is, the MS/MSS incurs handoff at the 20th second, 40th second, 60th second, and so on). The MSS has either a voice or video connection. In addition, both networks are with heavy traffic.

The throughput performances when the MS/MSS has a video connection are shown in Figs. 4(a) and 4(b). It's obvious that in the 802.11e network, the throughput varies significantly. The reasons are twofold: an MS contends channel to transmit data with others in IEEE 802.11e network; and the backoff value is randomly selected. Thus a



(a) Throughput performance of video connections in the IEEE 802.11e network



(b) Throughput performance of video connections in the IEEE 802.16e network

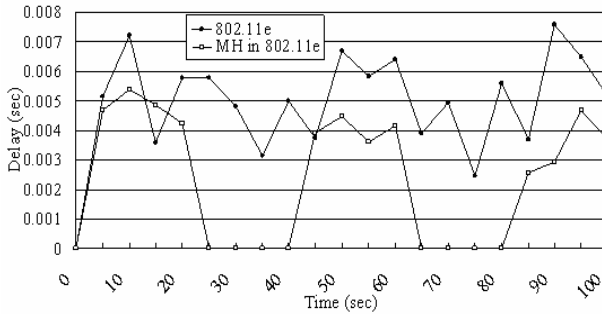
Fig. 4. Throughput performance in the heterogeneous network

connection's throughput performance is not guaranteed. In the IEEE 802.16e network, the throughput performances of the handoff connection and other existing connections differ little. The reason is that the BS performs CAC well, always allocates each connection's minimum QoS requirements first by setting T_1 timer, and then allocates residual bandwidth fairly by setting T_2 timer.

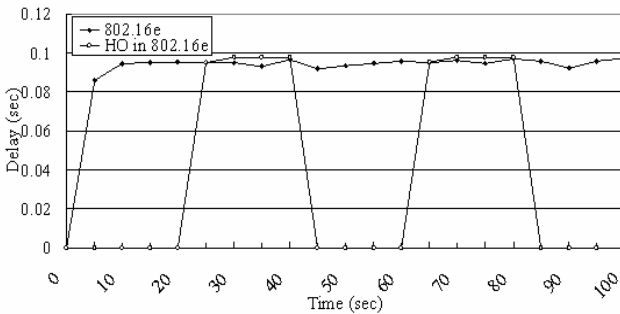
Figs. 5(a) and 5(b) show the average delay of video connections. Similarly to the throughput performance, the delay performance varies significantly in the 802.11e network and is stable in the IEEE 802.16e network. However, the delay in IEEE 802.16e network is larger than that in the IEEE 802.11e network. It is because the generated packets of an MSS are kept in the queue and wait for the transmission opportunity grant issued by the BS. On the other side, low average delay in the 802.11e network is caused by a fact the many packets are dropped after exceeding retry limits.

3.2.2 CAC Performance

In this experiment, we observe the effect of the implemented CAC module. We simulate an environment that the total minimum QoS requirements of connections exceed the provided network bandwidth.



(a) Delay performance of video connections in the IEEE 802.11e network

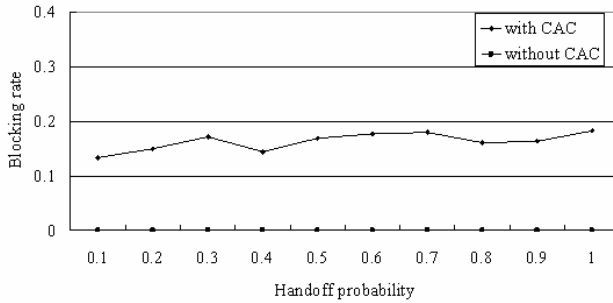


(b) Delay performance of video connections in the IEEE 802.16e network

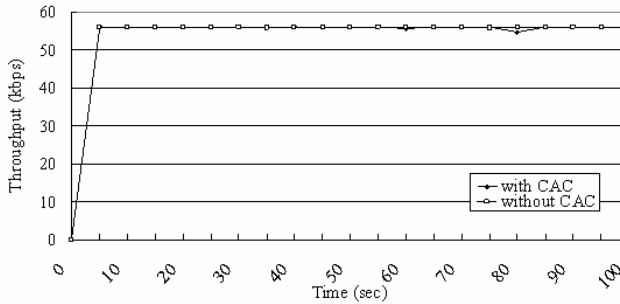
Fig. 5. Delay performance in the heterogeneous network

Fig. 6(a) shows the corresponding blocking rate. As expected that when implementing CAC, the handoff probability increases, and the blocking rate increases, too. However, the system guarantees the throughput performances of the existing and handoff connections (both UGS and nrtPS service classes), as shown in Figs. 6(b) and 6(c).

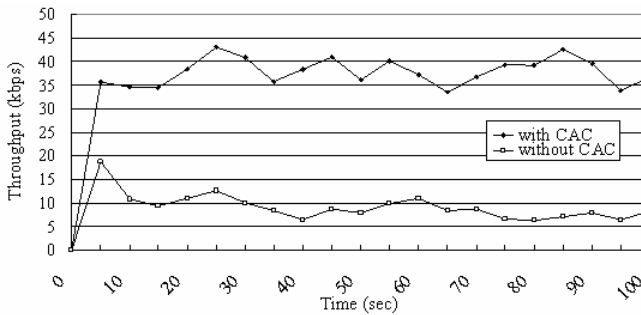
For the case that we do not implement CAC in an IEEE 802.16e network, every handoff connection is admitted to enter such a network, and its blocking rate is definitely zero, as shown in Fig. 6(a). However, its throughput performance may not be guaranteed. From Fig. 6(b), we found that no matter implementing CAC or not, UGS connections are not affected (since they are scheduled first), and their average throughput is 56Kbps (same as the demand). For nrtPS connections, their average throughput is less than 10 Kbps and thus their minimum QoS demands (i.e., 32 Kbps) are not satisfied due to the bandwidth shortage, as shown in Fig. 6(c).



(a) Blocking rate vs. handoff probability



(b) Throughput performance of UGS connections



(c) Throughput performance of nrtPS connections

Fig. 6. The observation of CAC impact in the IEEE 802.16e network

4 Conclusions and Future Work

In this paper, we implemented a QoS framework, including AC-SC mapping, CAC, and scheduling, for a heterogeneous network by using NS-2 simulator. The heterogeneous network consists of IEEE 802.11e and 802.16e networks. Our implemented modules support heterogeneous handoff. In addition, the simulation results show that the QoS demands of handoff connections are satisfied, and the CAC

performs well to eliminate the impact of handoff connections on other existing connections. The modified CAC reduces the blocking rate efficiently, too.

Our future work will integrate the signal-to-noise detection, mobility model, and signaling process of handoff into our QoS framework.

References

- [1] IEEE Std. 802.11e-2005, IEEE Standard for Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS) (2005)
- [2] IEEE 802.16e/D5-2004, IEEE Standard for Local and Metropolitan Area Networks-Part 16: Air Interface for Fixed Broadband Wireless Access Systems-Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands (September 18, 2004)
- [3] NS-2 simulator, <http://www.isi.edu/nsnam/ns/>
- [4] Jiang, C.-H., Tsai, T.-C.: Token bucket based CAC and packet scheduling for IEEE 802.16 broadband wireless access networks. In: IEEE CCNC 2006, pp. 183–187 (2006)

An Energy-Efficient MAC Design for IEEE 802.15.4-Based Wireless Sensor Networks

Yu-Kai Huang¹, Sze-Wei Huang¹, and Ai-Chun Pang^{1,2}

¹ Graduate Institute of Networking and Multimedia

² Department of Computer Science and Information Engineering
National Taiwan University, Taipei, Taiwan 106, ROC
{d94944009,r93944018,acpang}@csie.ntu.edu.tw

Abstract. This paper presents a new energy-efficient MAC design to improve the performance of IEEE 802.15.4-based wireless sensor networks. Our proposed mechanism adaptively determines the sleeping schedules of sensor nodes based on the network traffic load to achieve the balance of throughput and energy consumption. This mechanism consists of two phases: schedule exchange phase and schedule generation phase. In the schedule exchange phase, the schedule parameters are piggybacked in normal transmissions. In the schedule generation phase, sensor nodes adaptively determine the sleeping schedule from the schedule parameters. Eventually, the schedules of all sensor nodes converge to one schedule. The experimental results show that the proposed mechanism achieves sleeping schedule convergence and high energy efficiency.

Keywords: Power Saving, Energy Efficiency, Wireless Sensor Networks, IEEE 802.15.4, Low Rate Wireless Personal Area Networks (LR-WPANs).

1 Introduction

Wireless sensor networking is an emerging technology that has a wide range of potential applications including animal/plant habitation monitoring, target tracking, building monitoring, and robotic exploration. Such networks consist of large numbers of distributed nodes that organize themselves into multi-hop wireless systems. The sensor nodes are usually operated by batteries to simplify network deployment. With many nodes placed in their target environment, recharging batteries becomes more difficult, or even impossible. Therefore, energy efficiency has been a critical issue in wireless sensor networks.

The design of medium access control (MAC) plays an important role for energy efficiency of sensor nodes. In the MAC layer, most of the energy wastage comes from *idle listening*. Since sensor nodes do not figure out when it becomes the receiving side of a message from one of its neighbors, the sensor nodes have to turn on its radio receiver all the time and to keep listening even if the nodes are in the idle mode. The previous work has shown that *idle listening* consumes additional 50% to 100% of the energy [1]. To minimize the energy consumption caused by *idle listening*, an intelligent MAC algorithm shall be developed to make its best effort to turn off the radio when sensor nodes are idle.

The recent works such as SMAC [2] [3] and TMAC [4] have adopted a synchronized sleep/wakeup cycle to allow nodes to operate at low duty cycle for power saving. SMAC reduces idle listening by periodically putting nodes into sleep state. TMAC is an improvement of SMAC. In TMAC, if there is no activity in the vicinity of a node for a time T_A , the node will go to sleep for reducing idle listening. TMAC has the same performance as SMAC under constant traffic loads, but it saves more energy under a light-traffic condition. Also, TMAC uses the control packets RTS/CTS to exchange energy-consumption information. Both SMAC and TMAC can not adapt traffic variation well since its static design for fixed sleeping schedules of sensor nodes.

The release of IEEE 802.15.4, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)" [7] represents a milestone in wireless personal area networks. IEEE 802.15.4 is a new standard uniquely designed for low rate wireless personal area networks(LR-WPANs). It targets ultra-low complexity, cost, and power for low-data-rate wireless connectivity among inexpensive fixed, portable, and moving devices [8]. The standard also supports multi-hop packet delivery. Therefore, in comparison with 802.11, 802.15.4 is more suitable for wireless sensor networks.

Since IEEE 802.15.4 is a good alternative for wireless sensor networks, there are several issues about the sleeping schedule design. The system performance of a wireless sensor network is affected seriously by these issues.

– *Sleeping Schedule Adaption for Traffic Variation*

Since the traffic load of a wireless sensor network is not necessarily the same all the time, a fix sleeping schedule does not cope with the traffic variation. A duty cycle for heavy traffic loads results in energy wastage when the traffic becomes light, while the duty cycle for light traffic loads causes low throughput under increasing traffic loads. Particularly, in wireless sensor networks, the occurrence of emergencies generates heavy traffic in a short time such that the system performance seriously degrades. Therefore, it is required to adaptively determine the duty cycle according to the traffic situation.

– *The Occurrence of Multiple Schedules*

A sleeping schedule protocol establishes and maintains sleeping schedules for a wireless sensor network. When a node fails to hear an existing schedule, it shall create a new schedule for itself. In a large network, it is expected that a number of nodes create their own schedules. Therefore, multiple schedules occur in a large network [9]. Multiple schedules result in energy wastage and long latency for retransmission.

– *The Control Overhead*

When multiple schedules occur, the existing protocols usually use additional packets to exchange schedule information. The schedule exchange overhead causes additional power consumption. Therefore, it is necessary to simplify schedule exchange mechanism.

In this paper, we propose a new energy-efficient MAC design for IEEE 802.15.4-based wireless sensor networks. To consider the above issues, our MAC design adaptively determines the sleeping schedule based on the traffic load. To reduce the control overhead, devices piggyback schedule parameters embedded in data and acknowledgment packets. Therefore, the additional packets are avoided. Afterward, a device uses its neighbors' schedule parameters to adjust its own schedule. This mechanism converges multiple schedules to a single schedule gradually. The performance evaluation for our MAC design is conducted through the well known NS-2 simulator. Simulation results indicate that in terms of energy consumption and power efficiency, the proposed mechanism outperforms the legacy 802.15.4 MAC protocol.

The remainder of this paper is organized as follows: Section 2 describes the MAC protocol for IEEE 802.15.4. In Section 3, we formally define the problem, and propose an MAC design to adaptively determine the sleeping schedule for a wireless sensor network. In Section 4, the capability of the proposed MAC design is investigated under a series of experiments. Section 5 is the conclusion.

2 IEEE 802.15.4 MAC

The new IEEE standard, 802.15.4 defines the physical layer (PHY) and medium access control (MAC) sublayer specifications for low-rate wireless personal area networks (LR-WPANs), which supports simple devices that consume minimal power and typically operate in the personal operating space of 10 m or less. Thus, many corporations manufacture new wireless sensor boards for IEEE 802.15.4 [10, 11, 12]. The IEEE 802.15.4 defines two different modes for medium access: beacon-enabled mode and nonbeacon-enabled mode.

2.1 Nonbeacon-Enabled Mode

In nonbeacon-enabled mode of 802.15.4, unlike 802.11, the data transfer model is quite simple and does not need to use the additional control messages. When a device wishes to transfer data, it simply transmits its data frames using unslotted CSMA-CA mechanism. The receiver acknowledges the successful reception of the data by transmitting an optional acknowledgment frames.

The nonbeacon-enabled networks use an unslotted CSMA-CA channel access mechanism. Each time a device wishes to transmit data frames or MAC command, it shall wait for a random period. If channel is found to be idle, following the random backoff, the device will transmit its data. If channel is found to be busy, following the random backoff, the device shall wait for another random period before trying to access the channel again. Acknowledgment frames shall be sent without using a CSMA-CA mechanism.

In the nonbeacon-enabled networks, the coordinator do not use beacon frames to synchronize the attached devices, and any devices can communicate with any other device as long as they are in range of one another. Therefore, the nonbeacon-enabled networks are easy to enlarge the network scale and suitable

for a large scale sensor network. Applications such as industrial control and monitoring, wireless sensor networks, asset and inventory tracking, and intelligent agriculture would benefit from nonbeacon-enabled networks [14]. In the beacon-enabled mode, there is power-saving mechanism that the superframe can have an active and an inactive period, and all nodes may enter a low-power mode during inactive period [15]. However, there is no power-saving mechanism in the nonbeacon-enabled networks. Thus, we proposed an energy-efficiency MAC design for the nonbeacon-enabled networks, such that the nonbeacon-enabled networks achieve more power savings.

3 The Energy-Efficient MAC Design

In this section, we propose the energy-efficient MAC design for wireless sensor networks. Our MAC design includes two phases: *Schedule Exchange* and *Schedule Generation*. The *Schedule Exchange* phase operates during the awoken period of a sensor node. The phase is composed of two components. One is used to exchange schedule parameters among sensor nodes, and the other one counts the communication frequency representing the traffic load between two neighboring sensor nodes. To reduce the control overhead for parameter exchanging, the schedule parameters are piggybacked in data and acknowledgment packets.

The *Schedule Generation* phase operating in the sleeping period generates a new schedule for a sensor node, and slightly adjusts the schedule based on the traffic load. A new schedule is adaptively determined based on the schedule parameters and communication frequency derived in the *Schedule Exchange* phase. If there is any extreme traffic situation such as bursty packet arrivals, the new schedule will be adjusted to avoid starvation.

3.1 System Parameters

Before describing the details of our design, we elaborate the system parameters used in the *Schedule Exchange* phase.

In DATA packets

- W*: The waiting time of data packets. This parameter is used in schedule adjustment of the *Schedule Generation* phase, and is used to avoid the starvation. A source node transmits a data packet, and the destination node gets *W* embedded in the source node's packet. If the waiting time is larger than the predefined threshold, the destination node prolong the awaking period.

In ACK packets

- S*: The time that the node will sleep. The destination node sends the ACK packet with this parameter to the source node, and the source node knows when the destination node will sleep.

- Lw*: The duration that the node wakes up. The node records the neighbors' *Lw* in the neighbor list, and uses these *Lw* and the communication frequency to generate the node's new *Lw*.

• **L_s** : The duration that the node sleeps. The node records the neighbors' L_s in the neighbor list, and uses these L_s and the communication frequency to generate the node's new L_s .

Communication Frequency C_n : The number of communications between a node n and its neighboring node in the awoken period. Each node will count and record communication frequency of its neighboring nodes, and the communication frequency of each neighboring node becomes a weight for the generating of a new schedule.

3.2 Schedule Exchange Phase

In this phase, schedule parameters are exchanged, and the communication frequency is recorded. Every node maintains a neighbor list storing schedule parameters and the communication frequency of every neighbor. Schedule parameters are piggybacked in the DATA and ACK packets. When nodes send packets, schedule parameters are also exchanged among these nodes.

When a node receives a data packet, it records the waiting time of the source node. Then the node responds an acknowledgement packet back to the source node with its schedule parameters. The node receiving the acknowledgement updates the schedule parameters in the neighbor list. If other neighbors of the two node are awake, they can get the schedule parameters by overhearing the data and acknowledgement packets.

We briefly describe the schedule exchange operation through the following example (see Figure 11). In this example, there are three nodes in the sensor network and Figure 11(a) shows the sensor network topology. In Figure 11(b), node X sends a data packet with waiting time W to neighbor 1, and neighbor 1 receives the data packet and gets node X's waiting time W . At the same time, neighbor 2 overhears the data packet from node X and gets the node X's waiting time W . After received the data packet, neighbor 1 sends an acknowledgement packet with schedule parameters(S , L_s and L_w) back to node X, and node X receives the acknowledgement packet and updates neighbor 1's schedule parameters in the neighbor list. In the same way, Neighbor 2 will get neighbor 1's schedule parameters by overhearing the acknowledgement packet from neighbor 1.

3.3 Schedule Generation Phase

In this phase, we use schedule parameters mentioned in the previous section to generate and adjust the new schedule. This phase is to adaptively determine nodes' schedules based on the traffic load and converge multiple schedules to a single schedule. A node adopts a neighbor's communication frequency as the neighbor's weight, and average the weighted schedules of all neighbors as the node's new schedule. When a node enters the sleeping state, it computes the new schedule by the schedule parameters based on the communication frequency recorded in the neighbor list during the awoken period. Nodes adjust schedules in two situations. One is to cope with the extreme traffic situation after schedule

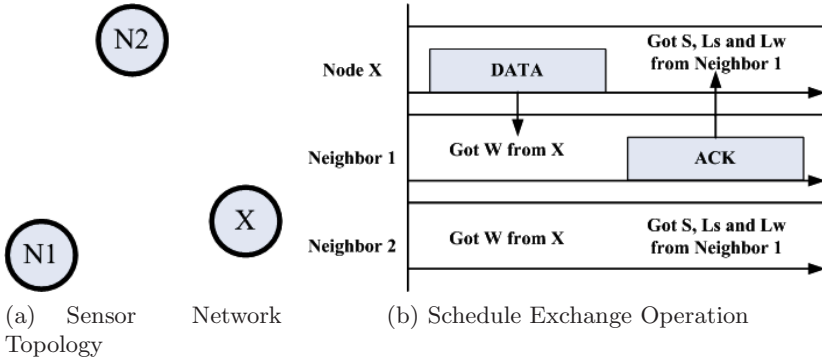


Fig. 1. An Example of Schedule Exchange

generation phase, and the other is to prolong the awoken period to avoid the starvation according to the waiting time W piggybacked in data packets from one of neighbors.

Schedule Generation Operation. To make multiple schedules converge to one schedule, nodes estimate the next time that neighbors sleep and wake up for schedule generation. The estimation method considers three cases, and we use schedule parameters(S, Ls and Lw) to derive two variables(P_n and X_n) for the three cases. P_n is a estimated time that the neighbor n will wake up in this or next schedule after the node wakes up. X_n is the duration of that the node should be awoken, and it is calculated by S, Ls and Lw for the neighbor n .

– Case 1: $S_n > S + L$.

In this case, S_n , the sleeping time of the neighbor n is larger than the time $S + L$ that the node X will wake up. Therefore, the node X directly set the time that the neighbor n will wake up in this schedule as P_n and the duration from that the node X will wake up to the sleeping time of the neighbor n as X_n (see Figure 2(a)).

$$P_n = S_n + Ls_n \tag{1}$$

$$X_n = S_n - (S + Ls) \tag{2}$$

– Case 2: $S_n < S + L$ and $S_n + Ls_n > S + L$.

In this case, S_n , the sleeping time of the neighbor n is smaller than the time $S + L$ that the node X will wake up but the time $S_n + Ls_n$ that the neighbor n will wake up in this schedule is larger than the time $S + L$. Therefore, the node X estimates P_n by increasing the duration of this schedule of the neighbor n , $Lw_n + Ls_n$. X_n is the duration from that the node X will wake up to the estimated sleeping time of the neighbor n (see Figure 2(b)).

$$P_n = S_n + Ls_n + Lw_n + Ls_n \tag{3}$$

$$X_n = S_n + Ls_n + Lw_n - (S + Ls) \tag{4}$$

– Case 3: $S_n + L_n \leq S + L$.

In this case, the time $S_n + L_n$ that the neighbor n will wake up in this schedule is equal to or smaller than the time $S + L$ that the node X will wake up. In other words, P_n will be the time $S_n + Ls_n$ that the neighbor n wakes up plus m times the duration of this schedule of the neighbor n until P_n is larger than $S + Ls$ and the value of m is equal to or larger than 0. X_n is the duration from that the node X will wake up to the last estimated sleeping time of of the neighbor n (see Figure 2(c)).

$$P_n = S_n + Ls_n + m \times (Lw_n + Ls_n) + Lw_n + Ls_n, \text{ where } m \geq 0 \tag{5}$$

$$X_n = S_n + Ls_n + m \times (Lw_n + Ls_n) + Lw_n - (S + Ls), \text{ where } m \geq 0 \tag{6}$$

To determine adaptively schedules based on the traffic, nodes use the communication frequency as the weight for the schedule generation. In the schedule generation phase, nodes generate the new schedule parameters by the weighted P_n and X_n that are multiplied by the communication frequency of the neighbor n (see equation 7,8 and 9).

$$Lw_{new} = \frac{\sum_n (X_n \times C_n)}{\sum_n C_n}, \text{ where } n \in \text{All Neighbors} \tag{7}$$

$$S_{new} = (S + L) + Lw_{new} \tag{8}$$

$$Ls_{new} = \frac{\sum_n (P_n \times C_n)}{\sum_n C_n} - S_{new}, \tag{9}$$

where $n \in \text{All Neighbors}$

Schedule Adjustment Operation. To cope with the extreme traffic situation, nodes adjust its schedule for better throughput and energy dissipation reduction. For example, when the traffic load becomes heavy suddenly, nodes should decrease the sleeping period and increase the awaking period for the throughput. Moreover, if there is no traffic between a node and its neighbors, the node should adjust its schedule by increasing the sleeping period and decreasing the awaking period for reducing energy dissipation. In the schedule adjustment, nodes adjust the sleeping period and the awaking period by slow-start algorithm [16]. Nodes increase the period exponentially (period = period × 2) until a predefined slow-start threshold is reached. Once the threshold is reached, the period is increased linearly (period = period + 1).

Another schedule adjustment is that a node prolongs the awaking period by waiting time W to avoid the starvation of its neighbor. When the node receives data packets from one of neighbors, it will get the waiting time W of the neighbor.

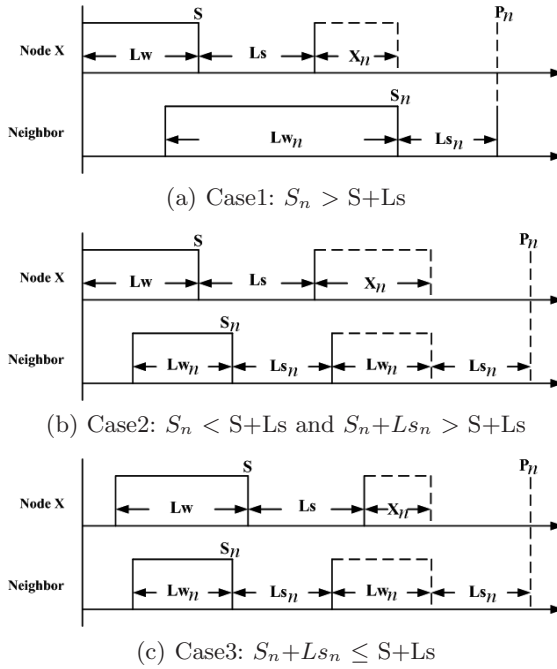


Fig. 2. P_n and X_n Estimation of Schedule Generation

If the waiting time W from the neighbor is larger than a predefined threshold, the node will prolong the awaking period immediately. On the other hand, if the waiting time W is smaller than the threshold, the node will not do the schedule adjustment by the waiting time W .

4 Performance Evaluation

This section investigates the performance of our energy-efficient MAC design for IEEE 802.15.4-based wireless sensor networks.

4.1 Simulation Environment

The simulation experiments are conducted through NS-2 [17] simulator, and the simulation time lasts for 5000 seconds. In the experiments, a sensor node generates normal messages with constant inter-arrival times, and generates emergency messages with 1 time per 100 seconds. Two simulation topologies are considered in the simulation. One is a simple chain with 10 nodes and the other is a random topology with 25 nodes. In the chain topology, the source node (i.e., the first node of the chain) sends packets to the destination node (i.e., the last node of

the chain). In the random topology, there are two source nodes, and the source nodes will send packets to the two destination nodes across the topology.

4.2 Input Parameters and Output Measures

We use IEEE 802.15.4 MAC implementation in NS-2 that follows the specification of IEEE 802.15.4 MAC layer. The input parameters are listed described as follows.

- **Normal traffic.** We change the traffic load by varying the inter-arrival period of messages. We assume that the message inter-arrival period varies from 1 to 10 seconds.

- **Emergency traffic.** We use the emergency traffic to cause the traffic unstable. We assume that an emergent message is generated per 0.2 seconds.

- **Energy Consumption.** To consider the energy consumption of a node, we measure the amount of time that the radio on each node has spent in different modes: sleep, idle, receiving or transmitting. The energy consumption in each mode is calculated by multiplying the time with required power listed in Table 1 to operate the radio in that mode.

Table 1. System Parameters

| Parameters | value |
|--------------------|-----------------|
| Initial Energy | 1000Joules |
| Idle Power | 712 μ Watts |
| Transmission Power | 31.32mWatts |
| Receiving Power | 35.28mWatts |
| Sleeping Power | 144nWatts |
| Number of devices | 10, 25 |

The output measures we adopt in the simulation are described as below.

- **Average Energy Consumption.** The average energy consumption is obtained by averaging the energy consumption of all nodes.

- **Power Efficiency.** Power efficiency is defined as the throughput achieved per unit of energy consumed, where the throughput represents the number of successfully delivered packets.

$$PowerEfficiency = \frac{Throughput(Packets)}{EnergyConsumption(Joules)}$$

- **Number of Schedules and Schedule Convergence Latency.** We observe the schedules of all nodes, and count the number of the schedules when we sample the network. The sampling interval is 10 seconds. As the number of the sampled schedules converges to 1, the convergence latency is also measured.

4.3 Numerical Results

Figure 3 shows the average energy consumption for the original nonbeacon-enabled network and our proposed MAC design under the chain and the random topologies. We first use the chain of 10 nodes for measurement. Figure 3 (a) indicates that the average energy consumption decreases as the message inter-arrival time increases. Moreover, the average energy consumption of the proposed MAC design is lower than the energy consumption in the idle state (Table 1). It indicates that we reduce the energy consumption of idle listening. In the random topology (Figure 3 (b)), the average energy consumption is still lower than that of the idle state. Since the latency of our MAC design is a little larger than the original one, it is tolerated in the wireless sensor network application.

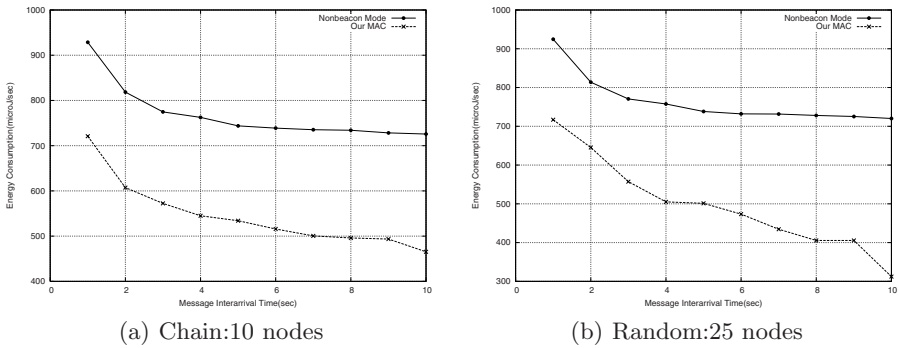
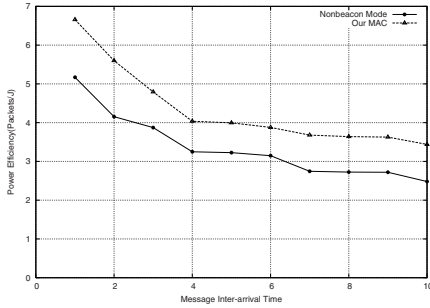


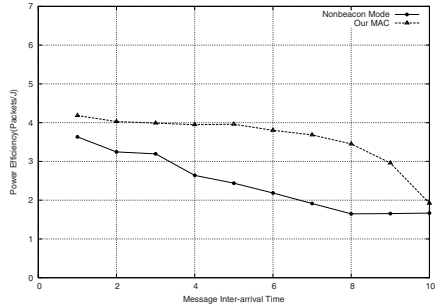
Fig. 3. Average power consumption

The output measure of power efficiency is shown in Figure 4 for the two topologies. In the chain topology, our MAC design achieves higher power efficiency than original nonbeacon-enabled network (see Figure 4 (a)). On the other hand, in the random topology, the power efficiency of the proposed MAC design is a little better than the original one (see Figure 4 (b)). Since many nodes in the boundary are often in the sleeping state in the random topology when the message inter-arrival time increases, the latency will increase and the throughput will be lower. Therefore, the power efficiency of our MAC design will be close to that of the original one.

Figure 5 indicates the number of the schedules in the network. When the emergency traffic occurs, multiple schedules will be generated, and the convergence latency will increase. After a while, the number of schedules in the network will converge to a single schedule gradually, and the latency will be reduced. In Figure 5 (b), since the nodes in the random topology are more distributive, multiple schedules occurring will make the latency increase seriously. Therefore, our MAC design solves this problem to reduce the latency. Although the emergency event causes the traffic unstable, our proposed MAC design will make multiple schedules converge to one schedule to reduce the latency.

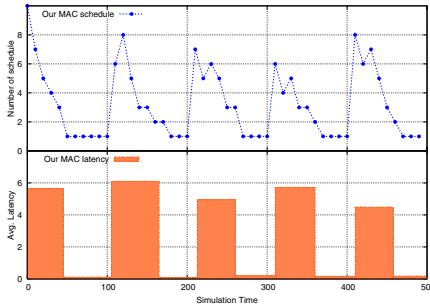


(a) Chain:10 nodes

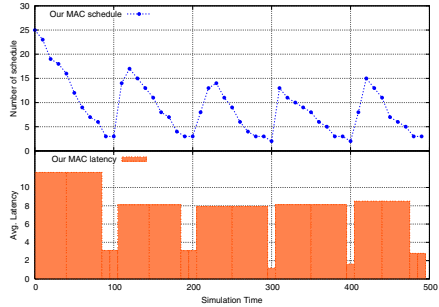


(b) Random:25 nodes

Fig. 4. Power efficiency



(a) chain:10 nodes



(b) Random:25 nodes

Fig. 5. Schedule Convergency

5 Conclusion

To improve the performance of the MAC protocol for IEEE 802.15.4-based wireless sensor networks in nonbeacon-enabled mode, this paper presents a new energy-efficient MAC design. Our MAC design adaptively determines the sleeping schedule of sensor nodes based on the network traffic load to achieve the balance of throughput and energy consumption. Our proposed MAC design consists of two phases: schedule exchange phase and schedule generation phase. In the schedule exchange phase, exchanging schedules is simple without extra overheads since the schedule parameters are piggybacked in DATA and ACK packets. In schedule generation phase, nodes adaptively determine the sleeping schedule by using the received schedule parameters. The experimental results show that the proposed MAC design achieves sleeping schedule convergence as well as high energy efficiency.

References

1. Stemm, M., Katz, R.H.: Measuring and Reducing Energy Consumption of Network Interfaces in Hand-Held Devices. IEICE Transaction on Communication (August 1997)
2. Wei Ye, J.H., Estrin, D.: An Energy-Efficient MAC Protocol for Wireless Sensor Networks. In: INFOCOM (June 2002)
3. Wei Ye, J.H., Estrin, D.: Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks. In: IEEE/ACM Transaction on Networking (2004)
4. van Dam, T., Langendoen, K.: An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks. SenSys (November 2003)
5. Tao Zheng, S.R., Sarangan, V.: PMAC: An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks. In: IPDPS (2005)
6. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Standard 802.11-1999 edition (1999)
7. 802.15.4-2003 IEEE Standard for Information Technology-Part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs) (2003)
8. Ed Callaway, P.G., Hester, L.: Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks. IEEE Communications Magazine (2002)
9. Yuan Li, W.Y., Heidemann, J.: Energy and Latency Control in Low Duty Cycle MAC Protocols. In: WCNC (2005)
10. Crossbow Technology Inc., MICAz wireless measurement system (June 2004), <http://www.zigbee.org>
11. Moteiv Corporation, Telos (Rev B) Datasheet (December 2004), <http://www.moteiv.com>
12. Intel iMote2 (February 2005), <http://www.intel.com/research/exploratory/mote.htm>
13. Timmons, N.F., Scanlon, W.G.: Analysis of the Performance of IEEE 802.15.4 for Medical Sensor Body Area Networking. In: IEEE SECON 2004 (2004)
14. Gutierrez, J.: On the use of IEEE 802.15.4 to enable wireless sensor networks in building automation. In: PIMRC 2004. Personal, Indoor and Mobile Radio Communications (2004)
15. Lu, G., Krishnamachari, B., Raghavendra, C.S.: Performance evaluation of the IEEE 802.15.4 MAC for low-rate low-power wireless networks. In: IPCCC 2004. Proceedings of the 23rd IEEE International Performance, Computing and Communications Conference (April 2004)
16. Kurose, J.F., Ross, K.W.: Computer Networks. Addison-Wesley, Reading (2003)
17. The NS-2 Simulator, <http://www.isi.edu/nsnam/ns/>

A Cross-Layer Signaling and Middleware Platform for Multi-interface Mobile Devices

Yung-Chien Shih¹, Kai-Cheng Hsu², and Chien-Chao Tseng¹

¹ Department of Computer Science, National Chiao Tung University,
1001 Ta Hsueh Rd., Hsinchu, Taiwan 300, ROC

² WiMAX Development Team, MediaTek Inc.,

No. 1, Dusing Rd., Hsinchu Science Park, Hsinchu, Taiwan 300, ROC
ycshih@csie.nctu.edu.tw, mojahsu@gmail.com, cctsen@cs.nctu.edu.tw

Abstract. This paper presents a middleware platform approach to provide Cross-layer Signaling and Network Event Notification mechanisms for network-aware applications. Because a mobile device may be equipped with multiple network interfaces to attach different network as it moves, a network-aware application running on the mobile device must react promptly to the changes of network environment. In order for the applications to detect network changes, the proposed middleware platform provides APIs for setting up network configuration and acquiring low-layer statuses. Therefore, an application can detect network changes promptly via Network Event Notification mechanism. We also use two network-aware applications, namely a Mobility Manager and a Modified Kphone, as examples to demonstrate the effectiveness of our middleware platform.

Keywords: Middleware, Cross-layer Signaling, Network Event Notification, Network-aware Application, Handover.

1 Introduction

With the advance in wireless techniques, mobile devices, such as *Personal Digital Assistant (PDA)*, smart phone, and tablet PC, has become a popular electronic product recently. A mobile device may be equipped with multiple wireless network interfaces, such as WLAN, GPRS, or 3G adaptors, to attach to different networks as it moves. Therefore, an application running on the mobile device may visit different networks and encounters the changes in bandwidth, delays, or IP addresses. In order to tackle network fluctuations, network-aware applications that can adapt themselves to the changes in network environment have now become a major research topic in recent years.

A network-aware application may need to issue system calls periodically to retrieve lower-layer statuses, such as IP addresses, entries of routing table, and connectivity of network adaptors. However, the network statuses normally do not change frequently. Periodical system calls with short intervals may waste system resources for getting the same information. On the other hand, with long intervals between system calls, the applications can not react to the changes of network environment promptly.

Furthermore, a mobile device with multiple network interfaces needs a mobility manager to monitor statuses of network adaptor and perform handover decision accordingly. In order to acquire the statuses and conduct a handover, a mobility manager needs to use system calls to communicate with underlying network protocol stacks, such as link layer, network layer, or transport layer. However, the use of system calls is not only error-prone but also not portable.

In order to solve above problems, we proposed a software platform for the development of network-aware applications. The platform adopts a middleware [1] approach and provides *Application Programming Interfaces (APIs)* for the application to use Cross-layer Signaling Mechanism. Based on the mechanism, an application can interact with the lower-layer network protocols to acquire network statuses and manage network interfaces. Besides, the platform also provides an Event Notification Mechanism for an application to register interested events of network changes so that the middleware can notify the application immediately when an event of interest occurs.

We also use network-aware applications, namely a Mobility Manager and a Modified Kphone [2], as two examples to demonstrate the effectiveness of our proposed platform. The Mobility Manager can monitor statuses of multiple network interfaces simultaneously and perform handover decision accordingly. The Modified Kphone is a *Voice over IP (VoIP)* application with a new handover decision module that can interact with our proposed platform.

The rest of this paper is organized as follows. In Section 2, we describe previous research on middleware and cross-layer design. Then in Section 3, we present the architecture of our middleware platform, including a Cross-layer Signaling Mechanism and an Event Notification Mechanism. We show the two examples of network-aware applications through our proposed platform in Section 4. Finally, Section 5 concludes the paper.

2 Related Work

The handover issues of a mobile device with multiple interfaces are popular research topic recently. Although Mobile IP [3] mechanism can achieve heterogeneous handover, a mobile device cannot perform the handover smoothly. A reason of this problem is that an application cannot acquire promptly the underlying statuses, such as network link up, link down or wireless signal strength, because each network protocol layer works independently with each other. Therefore, in recent years, several researchers have proposed middleware or cross-layer mechanism for the upper-layer application to acquire the statuses of the lower-layer protocols.

2.1 Middleware

Many researchers has proposed middleware approaches to supporting fast hand-off in heterogeneous network environment [4, 5, 6, 7, 8, 9]. In the research,

the middleware, provide interaction mechanisms among applications and lower-layer protocols. Accordingly, the middleware is situated between applications and the *Operating System (OS)* as shown in Fig. 1. It hides the complexity of error-prone system calls, OS APIs, from applications by encapsulating the complex system calls in into simple middleware APIs to provide high level functions for applications. Therefore, applications need not handle the connectivity and heterogeneity of the underlying networks. In stead, they can manage the networks and react to the changes of networks accordingly through middleware APIs.

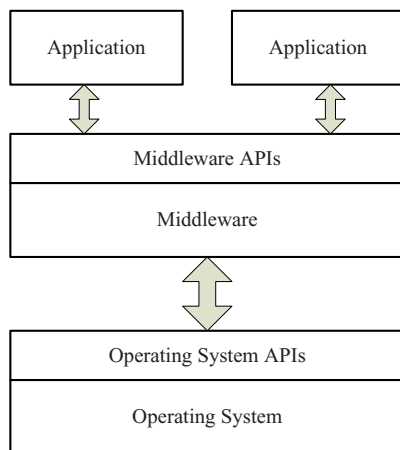


Fig. 1. The design concept of middleware was introduced in some research. The middleware is implemented between application and operating system, and then it provides high level functions for application to interact underlying protocol stacks.

If a programmer develops an application via the middleware, there are three benefits to develop applications via the middleware: easy porting, quick development and error avoidance. For application porting, because developing an application via middleware APIs can hide heterogeneity of OS, programmers need not modify any program codes when transplanting applications to another OS. For example, *Java Virtual Machine (JVM)* is one illustration of the middleware concept. It allows the same program code to run on different OSs. As for the application development and error avoidance, since middleware APIs provide simple interfaces for programmers to acquire and configure statuses of lower-layer protocols, programmers need not care for the details of system calls. Consequently, programmers can develop applications quickly and correctly.

Although many proposals adopted middleware concept to perform handover decision in a heterogeneous network environment, applications can not detect the changes of network environment immediately. We need other mechanisms to complete our middleware platform.

2.2 Cross Layer Design

According to the report of research [10], traditional network protocol that is used on mobile devices is not efficient because protocol stacks are working independently and thus those protocol stacks do not know statuses of other stacks. To solve the problem, the Cross Layer Feedback method has been mentioned in some previous work [11], [12]. This method provides an interaction mechanism for a protocol of a layer to share statuses with one of another layer. For example, a link layer protocol can share statuses with an application layer protocol and thus applications can adjust transmission rate according to the link statuses.

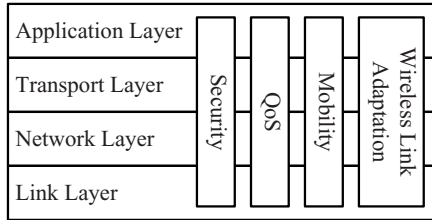


Fig. 2. The concept of Cross-Layer Notification Mechanism has been mentioned in past research. This mechanism allows a network protocol to inform other protocols the changes of network statuses proactively.

The Cross-Layer Notification Mechanism has been mentioned in past study [13]. This study suggested that a network protocol need a mechanism to inform other protocols about changes of network statuses. Therefore, cross-layer architecture, shown in Fig. 2, was proposed to satisfy needs of different applications, such as security, QoS or mobility requirement. For example of wireless link adaptation, when link quality of current attachment network is changed, the link layer will notify an application layer program of the link quality of each wireless adaptor or the transport layer of the maximum transmission rate. Furthermore, applications can inform the link layer to switch wireless adaptor.

2.3 Driver-Level Network Event Notification

The Driver-Level Network Event Notification Mechanism has been mentioned in our past research [14]. This mechanism adopted signaling mechanism to notify applications implemented in user space. Furthermore, it also modified OS scheduling algorithm to eliminate the needs for an application to issue system calls periodically to retrieve low-layer statuses. Implementation of the mechanism includes three major parts: (1) Event Notification, (2) Process Management and (3) Scheduler. In our implementation, before a process in the kernel space returns to the user space, the mechanism will check whether the registered events of this process occur or not. If the registered event occurs, the mechanism will call the corresponding procedure firstly. In this paper, we adopted our proposed event

notification mechanism and then modified some algorithms and data structures to satisfy requirements of our goal.

3 System Architecture

In this section, we will detail system architecture of the proposed middleware platform including Cross-layer Signaling and Event Notification mechanisms.

3.1 Middleware Platform and Cross-Layer Signaling

System architecture of proposed middleware platform can be divided into two major parts that include user space and kernel space. The middleware was implemented in user space and between application layer and underlying network layers and provided APIs for the network-aware applications, such as mobility manager and modified Kphone, to interact with underlying stacks of network protocol as shown in Fig. 3. For interaction between different network protocol stacks, the proposed middleware platform must provide Cross-layer Signaling Mechanism including statuses of underlying stacks acquisition, control messages dispatch and events notification for the applications. Therefore, the APIs are divided into three kinds including control, query and event interfaces. The control interface is used to notify underlying protocol stacks of changing statuses, such as adding or deleting entries of routing table, changing default gateway or attachment *Access Point (AP)*. The query interface is used to acquire specific status of underlying protocol stacks, such as wireless signal strength, IP address configurations or data transmission rate. The event interface allows the network-aware application to register interesting events and get event notification immediately when an interesting event occurs. Our implementation of event interface will be detailed in next subsection.

On the other hand, because the middleware must help the network-aware applications to interact with underlying protocol stacks, control and query messages received from applications need to translate into corresponding system calls. Therefore, we implemented the system call functions in proposed middleware, called Middleware Core, to interact with specific protocol layer located in kernel space. This part adopts cross-layer signaling design to order specific layer to do something and acquire statuses of specific layer. For example, an application can acquire wireless signal strength of WLAN adaptor or configure IP address directly. Furthermore, the Middleware Core will maintain some data structures, such as registered event tables and event queues, for applications to query or use.

To adopt proposed middleware platform, complex system calls can be reduced to simple APIs and thus an application can easy to use. Furthermore, to acquire and configure low-layer statuses via the Middleware APIs, a network-aware application can be developed quickly and error-less, and thus application developer can pay attention more to design handover policies.

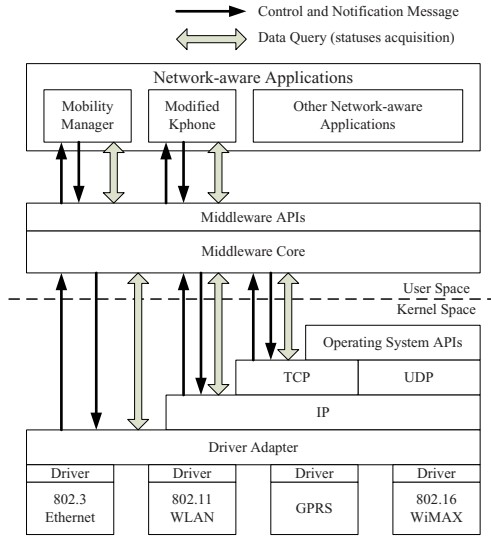


Fig. 3. The proposed middleware platform can be divided into two main parts: user space and kernel space. The middleware was implemented between the network-aware applications and underlying protocol stacks located in kernel space. Therefore, the Middleware APIs allow the network-aware applications to acquire and configure statuses of underlying protocol stacks.

3.2 Network Event Notification Mechanism

The event interface includes two kinds of method to notify the network-aware applications: synchronous and asynchronous process. In the synchronous process, a network-aware application must use Middleware API to initiate one or more than one event queues, and then register those queues and interesting events, called registered event, in Middleware Core as shown in Fig. 4. To illustrate this process, in the example program of synchronous process, an application must use the *win_event_init* function call and configure the parameter as “NULL” to initiate an event queue. Therefore, the application can use the *win_event_register* function call to register interesting events in Middleware Core, and then the Middleware Core will maintain a *Registered Event Table* including all interesting events of the application, such as LINK_UP, LINK_DOWN and NETDV_UP in Registered Event Table 1. When an event occurs, the Middleware Core will check all of Registered Event Tables and then push the event to corresponding event queues. Finally, the application can use *win_check_event* function call to poll event queues periodically.

In the asynchronous process, an application must create an event handler to prepare for event notifications. Using this process, the application can get event notification immediately when an event occurs. For example, an event handler that is named for “*my_event_handler*” must be created firstly, and then the application uses *win_init_event* function call and configures the parameter as the

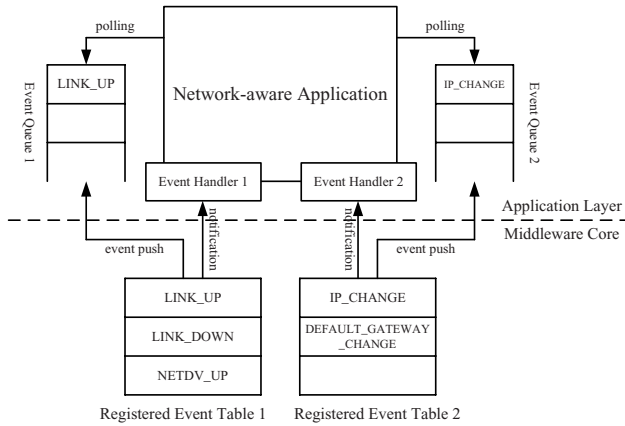


Fig. 4. There are two kinds of process of Event Notification Mechanism including synchronous and asynchronous. In the synchronous process, the Middleware Core will push event to event queue when an interested event occurs. On the other hand, in the asynchronous process, the Middleware Core will notify event handler when an interested event occurs and then the network-aware application can know the occurrence of an event immediately.

handler name to initiate asynchronous process as shown in example program of asynchronous process. Therefore, the application can use `win_event_register` function call to register interesting events similarly. The Middleware Core will dispatch event notification to corresponding event handlers when an event occurs so the application knows event occurrence and the corresponding handler procedure will run immediately.

In the kernel level, we adopted the Driver-level Network Event Notification Mechanism that is developed by our research partner and mentioned in Section 2 to support our Event Notification Mechanism. Furthermore, we had added novel events, such as `ROUTING_TABLE_CHANGE`, to extend the notification mechanism so the middleware platform can be used to help network-aware application that it gets interesting event notifications correctly and immediately.

An Example Program of Synchronous Process

```
event_descriptor = win_event_init(NULL);

win_event_register(event_descriptor, NETDEV_UP);
win_event_register(event_descriptor, IP_CHANGE);
...

if(win_check_event(event_descriptor, wevent)
    == R_HAVE_EVENT) {
    ...
}
```

An Example Program of Asynchronous Process

```

void my_event_handler(struct win_event* wevent) {
    printf(Event Happen!!\n);
}

int main() {
    ...
    event_descriptor = win_event_init(my_event_handler);
    win_event_register(event_descriptor, NETDEV_UP);
    win_event_register(event_descriptor, IP_CHANGE);
    ...
}

```

4 Network-Aware Application

Based on our middleware platform, a program developer can develop a network-aware application quickly and easily. In this section, we will demonstrate two network-aware applications including Mobility Manager and Modified Kphone.

4.1 Mobility Manager

A mobility manager for mobile device should include three major functions: display of network status, network configuration and handover policy. Therefore, we implemented the Mobility Manager application that used Middleware APIs to acquire and configure statuses of underlying protocol stacks. For example, in the Fig. 5, wireless signal strength of APs can be displayed on a single graphic interface. Furthermore, a user of mobile device can use a graphic configuration interface to set attachment AP and choose acquisition method of IP address as shown in Fig. 6.



Fig. 5. This graphic interface will display wireless signal strength of APs that a mobile device can attach. For example, this figure displays three signal strengths of AP including WL1, WIN and wireless_b.

For mobile device handover, we need to know the changes of network environment and then mobile device chooses another network to attach according user preference if current attachment network is unreachable or low quality. In

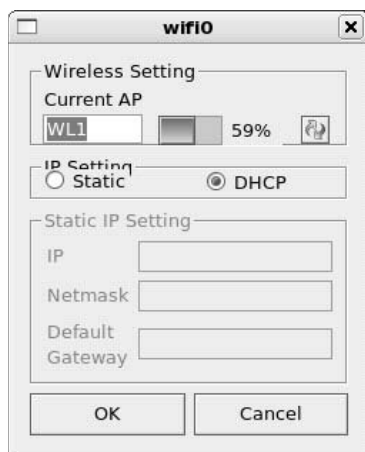


Fig. 6. This graphic interface allows user of mobile device to configure current attachment AP and choose acquisition method of IP address, such as static or DHCP

our implementation, the Mobility Manager allows user to choose manual or automatic handover and to assign preferred interface as shown in Fig. 7. User can configure a profile of handover policy that records when handover can be performed and what something is needed to do in handover, if the Mobility Manager be configured automatic handover mode.



Fig. 7. User of a mobile device can use this graphic interface to choose manual or automatic handover and to assign preferred interface

In summary, a mobile device can acquire network statuses, such as current IP address and signal strength of APs, and configure those network statuses easily if the Mobility Manager application runs on this mobile device. Furthermore, the mobile device can make handover decision automatically according network environment changes, such as link quality or reachable network, and user preference.

4.2 Modified Kphone

The Modified Kphone is another example of network-aware application that is sourced from a VoIP application called Kphone and is modified to perform handover via the Middleware APIs. We need to program some new procedures to make handover decision because the original Kphone application cannot support handover. In the Kphone communication, a *Mobile Node (MN)* and a *Correspondent Node (CN)* are transmitting voice data via *Real-time Transport Protocol (RTP)* packets to another. We need to ensure that *Synchronization Source Identifier (SSRC)* in RTP header is identical when the MN changes its IP address because same SSRC in RTP header implies same connection between MN and CN.

In our implementation of Modified Kphone, we divided handover procedure into four steps as shown in Fig. 8. First, a MN receives a network event notification, such as wireless signal strength below a threshold, and then it triggers network layer handover that includes changing attachment network, acquiring a new IP address and configuring default gateway. Second, the MN uses the new IP address and original SSRC to send Re-invite message to CN. Third, the CN will change destination IP address of sending packets according source IP address of received packet and the SSRC when it receives the Re-invite message. Finally, the CN will send ACK message to the MN and thus an application layer handover is completed.

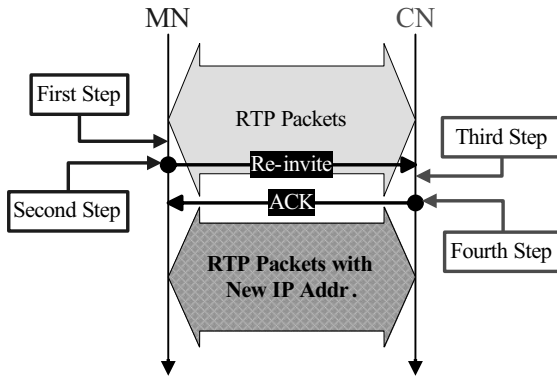


Fig. 8. The handover procedure of Modified Kphone can be divided into four steps. If a network event notification be sent to Modified Kphone and it decides to perform handover, this handover procedure that includes first, second, third and fourth step will be run.

In summary, our Modified Kphone application can perform handover quickly and correctly because the middleware platform can provides layer-2 trigger and some detail statuses for an application. Furthermore, a program developer can

pay attention more to design of handover policies as a result of the middleware platform provides several mechanisms for the developer to implement applications.

5 Conclusion

In this paper, we designed and implemented a middleware platform that includes Cross-layer Signaling and Network Event Notification mechanisms. The middleware was implemented in user space and then it provided Middleware APIs for applications to configure and acquire statuses of underlying protocol stacks. Based on Cross-layer Signaling mechanism, control and query messages can order each protocol stack to do something directly. Beside, the Network Event Notification can help application that it is aware of changes of network environment immediately.

We also demonstrated two examples of network-aware application that include Mobility Manger and Modified Kphone. Those examples illustrated two kinds of Event Notification method and how to use in our middleware platform. According our illustration, if a network-aware application is developed via our middleware platform, this application can be developed quickly and easily.

In future works, we will continue to extend novel network events when a new type of network adaptor is created. Furthermore, we consider developing a handover analysis tool via the middleware platform and then the tool can help programmer to determine cause of handover delay.

References

1. Bakken, D.: Middleware, <http://www.eecs.wsu.edu/~bakken/middleware.pdf>
2. Kphone Project, <http://sourceforge.net/projects/kphone>
3. Perkins, C.: IP Mobility Support for IPv4. IETF RFC3344, Nokia Research Center (August 2002)
4. Sun, J., Riekkki, J., Jurmu, M., Sauvola, J.: Adaptive Connectivity Management Middleware for Heterogeneous Wireless Networks. IEEE Wireless Communications (2005)
5. Sun, J., Tenhunen, J., Sauvola, J.: CME: a middleware architecture for network-aware adaptive applications. In: Proceedings 14th IEEE PIMRC 2003, Beijing, China (2003)
6. Hawick, K.A., James, H.A.: Wireless Issues for a Mobility Management Middleware. In: CCN 2002 (August 2002)
7. Tian, Y., Frank, S., Tsoussidis, V., Badr, H.: Middleware Design Issues for Application Management in Heterogeneous Networks. In: ICON 2000. Networks 2000 (2000)
8. Li, B., Nahrstedt, K.: A Control-Based Middleware Framework for Quality of Service Adaptations. IEEE Journal of Selected Areas in Communication 17(9), 1632–1650 (1999)
9. Kreller, B., Park, A.S.B., Meggers, J., Forsgren, G., Kovacs, E., Rosinus, M., Siemens, A.G.: UMTS: A Middleware Architecture and Mobile API Approach. IEEE Personal Communications (April 1998)

10. George, X., George, C.P.: Internet Protocol Performance over Networks with Wireless Links. *IEEE Network* 13(4), 55–63 (1999)
11. Clark, D.D.: The Structuring of Systems using Upcalls. In: *ACM Symposium on Operating Systems*, pp. 171–180 (1985)
12. Cooper, G.H.: The Argument for Soft Layer of Protocols. In *Tech. Rep. Tr-300*, Massachusetts Institute of Technology, Cambridge (May 1983)
13. Carneiro, G., Ruela, J., Ricardo, M.: Cross-Layer Design in 4G Wireless Terminals. *IEEE Wireless Communications* 11(2), 7–13 (2004)
14. Chou, T.J.: Design and Implementation of Driver-Level Network Event Notification Mechanism in Linux. In *Thesis in Wireless Internet Lab.*, National Chiao Tung University, Hsinchu, Taiwan (2005)

Enhanced Sleep Mode Operations for Energy Saving in IEEE 802.16e*

Sixian Zheng, Kuochen Wang, Shiao-Li Tsao, and Pochun Lin

Department of Computer Science
National Chiao Tung University
Hsinchu, 300, Taiwan
kwang@cs.nctu.edu.tw

Abstract. The broadband wireless access (BWA) network, such as IEEE 802.16e, becomes more and more popular in recent years. According to the IEEE 802.16e specifications, mobile subscriber stations (MSSs) with energy constraints are allowed to switch to the sleep mode to reduce their power consumption. Considering a number of service connections on the MSS with different traffic characteristics and requesting different power saving classes, the MSS may not be able to sleep and save energy due to improper schedules of sleep operations for service connections. In this paper, an *enhanced longer common sleep time* (E-LCST) scheme is proposed and it first schedules real-time packets together in less number of frames without violating their delay constraints. After the listen and sleep frames are determined for transmitting real-time packets, the proposed scheme then considers non-real-time packets and schedules them into the existing listen frames if the resources are available. Therefore, MSSs can have more sleep frames and save the energy. Simulation results have shown that the proposed E-LCST performs 33% to 68% better than the conventional IEEE 802.16e Standard in terms of percentage of sleep periods, which reflects power consumption. Although, the proposed E-LCST introduces a little bit more delay, the QoS requirements of real-time connections are still met.

Keywords: Energy consumption, Energy efficiency, IEEE 802.16e, Power saving, Sleep mode, WiMax.

1 Introduction

The IEEE 802.16 standard [1] initially considers fixed broadband wireless access (BWA) in which all subscriber stations (SSs) are fixed nodes. The emerging IEEE 802.16e standard [2] enhances the mobility function so that mobile subscriber stations (MSSs) can be supported. The energy saving of mobile devices thus becomes a very important issue, because mobile devices are usually battery-operated. In the IEEE 802.16e, a base station (BS) serves as a control point which schedules radio resources for all MSSs attached to the BS. For MSSs, there are two operation modes, i.e. normal

* This work was supported by the NCTU EECS-MediaTek Research Center under Grant Q583.

mode (or called active mode) and sleep mode. The normal mode is the state that an MSS can transmit and receive data with the BS at anytime. For sleep mode, an MSS has to negotiate the sleep mode parameters with the BS. Then, the MSS can switch between sleep modes which the MSS is unavailable from the BS's perspective and listen modes which the MSS can send and receive packets from the BS. The sleep mode operation intends to minimize the power usage of MSSs [2].

When a connection is established, an MSS can switch to the sleep mode if there is no packet to transmit. The specification defines the sleep mode operation. In the sleep mode operation, the time is divided into fixed sizes, called frames. A frame is the basic unit of time to send, receive and listen. Before entering the sleep mode, the MSS have to send a sleep request frame to the BS. If the MSS gains the approval from the BS, then it will enter the sleep mode. When an MSS enters the sleep mode, it sleeps during the sleep window and wakes up at the listening window to receive the MOB-TRF-IND (mobile traffic indication) message. If there is no buffered packet for itself, it sleeps again until the next listening window. The actions of sleeping and listening with updated size of sleep window are repeated until there is buffered data for the MSS to transmit. The MSS also wakes up from the sleep mode when the MSS has data to transmit to the BS.

The IEEE 802.16e defines three power saving classes for different applications which generate different traffic characteristics. Power saving class is a group of connections that have common demand properties [2]. For different connections between the BS and the MSS, there are different QoS requirements. So we group different connections into different power saving classes to satisfy their QoS requirements. The type I power-saving class specifies that an MSS sleeps for a period, wakes up to listen for incoming packets, and repeats sleep and listen operations. If there is no packet to send or receive during a listen window, an MSS doubles the window for the next sleep. This power-saving class is suitable for the connections of web browsing or data access services such as BE (best-effort) or NRT-VR (non-real time-variable rate) service. The type II power-saving class requires an MSS to repeat the sleep and listen on a round-robin basis, and the sleep and listen windows are fixed. This sleep mode is appropriate for real-time connections such as VoIP and video streaming services that have packets to send or receive periodically. It is suitable for connections of UGS (unsolicited grant service) or RT-VR service. Based on the type II sleep mode, an MSS only needs to wake up to send or receive packets in those listen windows without violating the QoS of the real-time connections. The type III power-saving class defines the length of a sleep window, and an MSS sleeps for that window and then returns to the normal operation. Fig. 1, Fig. 2, and Fig. 3 illustrate examples for the three power-saving classes.

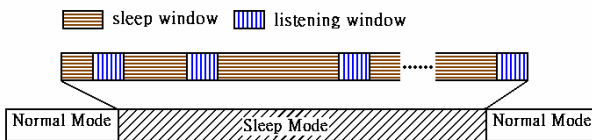


Fig. 1. Operation of power saving classes of type I

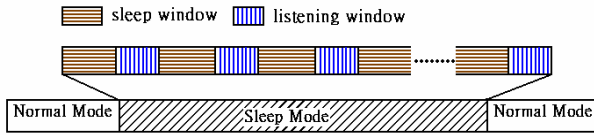


Fig. 2. Operation of power saving classes of type II

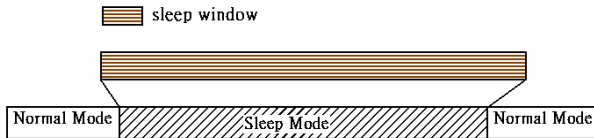


Fig. 3. Operation of power saving classes of type III

2 Problem Statement and Related Work

There are usually many different connections on an MSS. To switch to sleep mode and save power, an MSS has to consider sleep windows of all service connections. We define the notation “sleep time” as the total periods of sleep windows in the sleep mode for one connection and the notation “common sleep time” as the common periods of sleep time among several connections. Fig. 4 is an example of sleep mode operation with two power saving classes (type I and type II). Each connection has its own sleep time indicated by sleep windows. In the state of the MSS, the periods which are marked as “Sleep Time” is the common sleep time between the two connections. The periods of sleep time is the actual time duration for the MSS to enter the sleep mode to save power. Note that in Fig. 4, each connection has more sleep time in its own sleep mode operation. However, the common sleep time that the MSS can enter the sleep mode is much less than the sleep time of each connection. This is because the listening windows are not at the same time periods between two connections.

To improve the energy efficiency, the MSS needs to prolong the sleep time. The basic idea of the proposed approach is to reduce the number of listening windows by grouping packets that are originally scheduled to send in multiple listening windows, and send them in one single listening window without violating the delay constraints of different connections so as to lighten the effect of dispersive listening windows.

Several researches focused on the performance analysis of sleep mode operation in the IEEE 802.16e. However most of them only concentrated on the performance analysis of power saving classes of type I. In [3] [4], the authors proposed a model for performance analysis of the sleep-mode operation for energy saving considering both incoming and outgoing frames of MSSs. In [5], it examined the sleep mode operation in IEEE 802.16e in terms of the dropping probability and the mean waiting time of packets in the queue buffer of BS. In [6], they proposed two scheduling algorithms (PS and AS) for power saving classes of type II connections. The schemes minimize

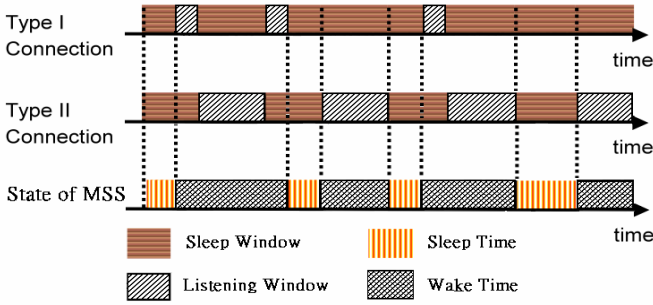


Fig. 4. Example sleep mode operation with two power saving classes

the power consumption of an MSS and also guarantee the requirement of QoS. They group packets into the same frame to reduce the number of listening windows. It groups two type II packets into a single frame. The number of listening windows is reduced and the sleep periods increase. As a result, there is more sleep time for the MSS to enter the sleep mode and save more power.

3 Proposed Energy Saving Schemes

There are usually more than one service connections on an MSS. From Fig. 4, we know that if there is more than one connection, the total common sleep time may decrease, because the total common sleep time is the common periods of sleep time among all connections. If we can reduce the number of listening windows in any connection, we can have more total common sleep time among connections, thus have more sleep time to save power. In this paper, we propose two energy saving schemes to increase the length of common sleep time and to enhance the energy saving of sleep mode operation. Our schemes are suited to an environment that has both power saving classes of type I and type II connections. In our schemes, we didn't consider the power saving classes of type III, which is for multicast connections, since we focus on the unicast connections only.

The first scheme is called *Longer Common Sleep Time (LCST)*. Because the power saving classes of type II (for UGS, RT-VR) is time-sensitive, we only modify the operation of the power saving classes of type I to have more common sleep time. For type I connections, the MSS wakes up to listen the traffic indication message at each listening window. The MSS returns to sleep mode again when there is no buffered data in the BS. The basic idea of our LCST scheme to removes the listening windows from the power saving classes of type I connections and the traffic indication messages of power saving classes of type I will be handled during the listening windows of power saving classes of type II connections. The reason to do so is because the power saving classes of type I is for connections of BE and NRT-VR, which are time-insensitive.

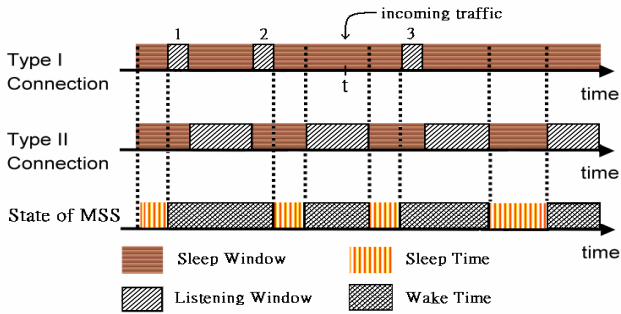


Fig. 5. Original scheme of power saving classes

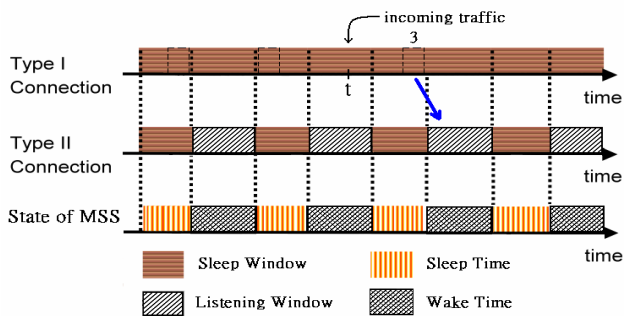


Fig. 6. Proposed method of power saving classes

In Fig. 5, there are three listening windows in the type I connection. The MSS has to wake three times to listen the traffic indication message. If there is only one data coming at time t , in the first and second listening windows, the MSS needs to wake up and then return to sleep right away. We can have longer common sleep time if we can keep sleeping at these two listening windows. In Fig. 6, the proposed LCST method removes the listening windows from the power saving classes of type I connection and the traffic indication message transmitted by the BS will be handled during the listening windows of type II connection. For example, in Fig. 6, the incoming traffic at time t will be handled during the third listening window of type II connection. The advantage of our LCST scheme is that for type I connections, the MSS doesn't need to wake up at all to listen the traffic indication messages from the BS. This method reduces the effect of type I connections on common sleep time, and the MSS shall have longer sleep time to enter the sleep mode. On the other hand, the method uses the periodic characteristic of type II connections to read type I traffic indication messages if any. Note that the type II connection wakes up in a fixed period, so the delay of type I connections can be bounded. In summary, this method eliminates of the listening windows of type I connections to save more power while type I connections have bounded delays.

Besides the LCST, we combine the idea of [6] to enhance the LCST scheme. We called it enhanced LCST (E-LCST). This E-LCST scheme groups several type II packets into a single packet in one connection to reduce the number of frames that need to transmit them from BS to MSS. In this way, the sleep periods of this connection can be increased. As a result, the MSS can have more common sleep time among different connections to enter the sleep mode and save more power. The proposed two schemes, LCST and E-LCST are compatible with the original IEEE 802.16e standard in terms of no change of MSSs and no change of the communication mechanism between BS and MSS. The only requirement is that the BS needs to be aware of LCST and E-LCST in order to set appropriate values of T_{min} and T_{max} . For the LCST, assume a type I connection of the MSS sends a request of sleep mode operation to the BS. Then, if the BS permits the request, it will set the parameter T_{init} to a very large number. For this type I connection, the MSS will not wake up periodically to listen to the traffic indication message. If there are buffered packets for the type I connections in the BS, the BS can transmit the packets to the MSS via the frames of type II connections. If the data size of power saving classes of type I is small enough, we can use the unused frame space of a type II connection to transmit. Otherwise, the BS will transmit the data to the MSS in the next frame and the MSS will stay awake to receive the data. For the E-LCST, the BS may group several type II packets that are to be sent in separate frames, into a single frame for transmitting later. In this situation, the BS only needs to adjust T_{min} to allow the MSS to sleep longer. Again, for E-LCST to work, the only requirement is the BS needs to be aware of E-LCST. No other changes are necessary in the MSS or the communications between BS and MSS.

Our schemes are designed for an environment with both power saving classes of type I and type II connections. If there are many connections of type I and less connections of type II, our schemes may not achieve a good performance. Because if too many buffered data have to be transmitted with type II frames, the average packet delay of type I connections will be extended and the advantage of using unused frame space of type II connections will not work well.

4 Simulation Results and Discussion

We wrote a C++ program to simulate and evaluate the performance of LCST, E-LCST and the sleep mode operation in the IEEE 802.16e in terms of the percentage of sleep periods and average packet delay. The percentage of sleep periods, which reflects the power consumption of an MSS, is defined as (number of sleep frames) / (number of sleep frames + number of listening frames + number of awake frames). The average packet delay is the average elapsed time from the time that a packet enters the BS to the time that the packet completes its transmission to the MSS. The simulation environment is similar to that in [6]. The duration of an OFDM frame is assumed 5 ms, and the maximal data rate that a BS can offer an MSS is assumed 1600 kbps. That is, the frame length is 1000 bytes. Eight different traffic connections were defined and the parameters of them are described in Table 1 and Table 2. Some parameters were referred from [4] and [6] and we modified part of them to demonstrate the energy efficiency of our proposed schemes in every respect.

Connections A, B, C and D are power saving classes of type I, and connections E, F, G and H are power saving classes of type II. The main difference between connections in each type is the variations of packet size and interval of packet arrival. This is to evaluate the performance under different traffic loads. The values of packet size and interval of packet arrival for each packet in type I connections were randomly generated from the ranges specified in Table 1.

Table 1. Parameters of type I connections

| Connection | A | B | C | D |
|---------------------------------|----------|----------|-----------|-----------|
| Type | I | I | I | I |
| Packet size (Bytes) | 1~1000 | 1~1000 | 1000~2000 | 1000~2000 |
| Sleep Period (ms) | [5, 320] | [5, 160] | [5, 320] | [5, 160] |
| Interval of packet arrival (ms) | 1~350 | 1~180 | 1~350 | 1~180 |

Table 2. Parameters of type II connections

| Connection | E | F | G | H |
|---------------------------------|-----|-----|-----|-----|
| Type | II | II | II | II |
| Packet size (Bytes) | 160 | 160 | 800 | 800 |
| Interval of packet arrival (ms) | 20 | 30 | 20 | 30 |
| Delay constraint (ms) | 100 | 100 | 100 | 100 |

In Fig. 7, it shows the percentages of sleep periods using the three different schemes (802.16e, LCST and E-LCST). The higher percentage of the sleep period is, the longer common sleep time that an MSS can enter the sleep mode and save more power. The notation A+E means that there are only two connections, A and E. It is a simple traffic environment. By increasing the number of connections, the traffic environment becomes more complex. We found that if the traffic environment becomes more complex, the percentage of sleep periods will become smaller in all the three schemes. In all cases, both the proposed two schemes performed better than the IEEE 802.16e. In Fig. 7, it shows that the percentages of sleep periods of LCST and E-LCST are 14% to 50% and 33% to 68% more than IEEE 802.16e, respectively.

The overhead of the proposed schemes (LCST, E-LCST) is that they have longer average delay than the scheme of IEEE 802.16e. The reason is that we delay the listening windows and reduce the number of listening windows. The buffered data in the BS are sent only after the listening windows of type II connections. However, we bounded the delay. The listening windows were postponed by the evaluation with delay constraint of type II connections. For connections of power saving classes of type II, we also guarantee their QoS. For the connections of power saving classes of type I, we wouldn't make their average delay longer than the delay constraint of type II.

Fig. 8 shows the average packet delay in different traffic environments. For type I (T1) connections, the LCST has 6% to 31% longer average packet delay than the IEEE 802.16e scheme and the E-LCST has 71% to 77% longer average packet delay than the IEEE 802.16e scheme. For type II (T2) connections, the LCST has the same average packet delay as the IEEE 802.16e scheme since the LCST did not modify the sleep mode operation of type II connections. The E-LCST has 84% to 88% longer

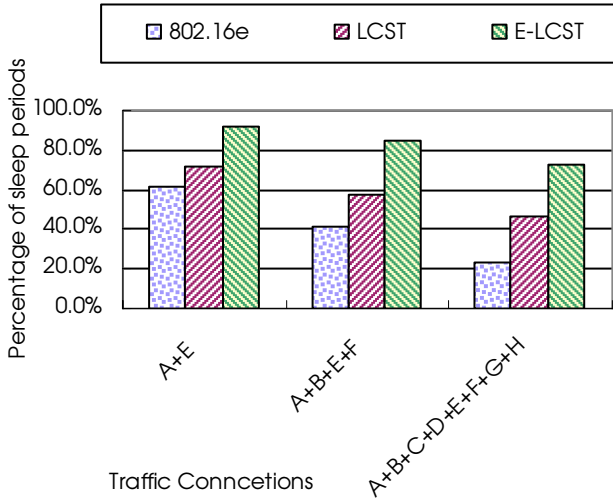


Fig. 7. Percentage of sleep periods under the loose delay constraint

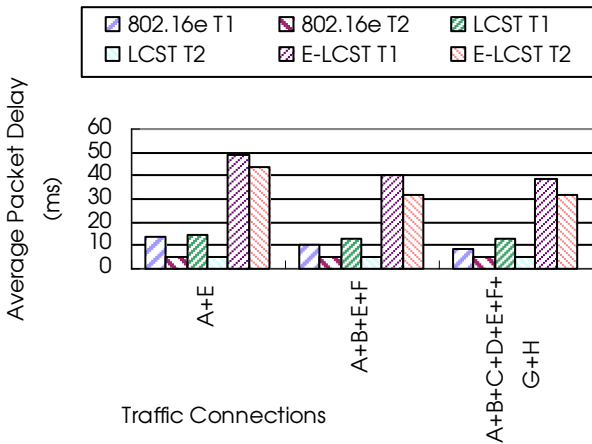


Fig. 8. Average packet delay under the loose delay constraint

average packet delay than the IEEE 802.16e scheme. The IEEE 802.16e scheme achieves the lowest packet delay, because its MSS wakes up more frequently to transmit packets. Nevertheless, the simulation results indicate that all schemes, no matter type I or type II connections all satisfied the QoS requirement in terms of delay constraints specified in Table 2.

Since we can bound the average packet delay under the delay constraint of type II connections in our schemes, here we present another simulation results of the percentage of sleep periods and average packet delay with a tight delay constraint in Fig. 8 and Fig. 10, respectively. The parameters of connections E', F', G', and H' are

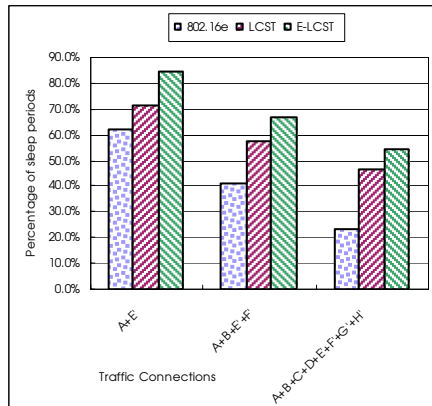


Fig. 9. Percentage of sleep periods under the tight delay constraint

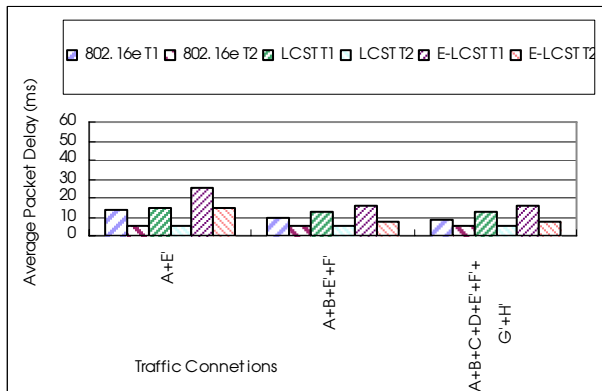


Fig. 10. Average packet delay under the tight delay constraint

the same with connections E, F, G and H respectively, except the delay constraint. We changed from the loose delay constraint of 100 ms to a tight delay constraint of 30 ms. The simulation results still show that the LCST is 14% to 50% better than IEEE 802.16e and the E-LCST is 26% to 57% better than IEEE 802.16e in terms of the percentage of sleep periods. The average packet delay of the LCST is still the same as the IEEE 802.16e scheme, but the average packet delay in the E-LCST decreases obviously. This is because the value of delay constraint affects the length of sleep interval in type II connections. For type I connections, the E-LCST has 38% to 44% longer average packet delay than the IEEE 802.16e scheme. For type II connections, the E-LCST has 33% to 67% longer average packet delay than the IEEE 802.16e scheme. If the delay constraint is set smaller, the average packet delay in the E-LCST will become smaller. This is because we use the delay constraint to calculate the number of packets that can be grouped into a single frame for transmitting and thus to guarantee the QoS.

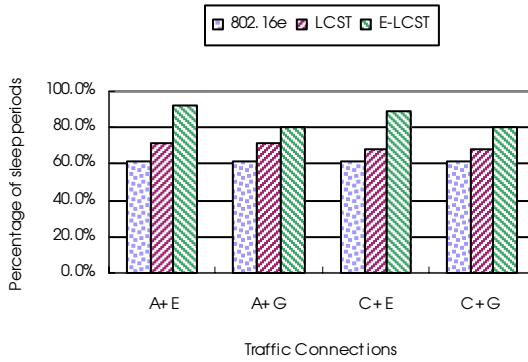


Fig. 11. The effect of packet size on percentage of sleep periods

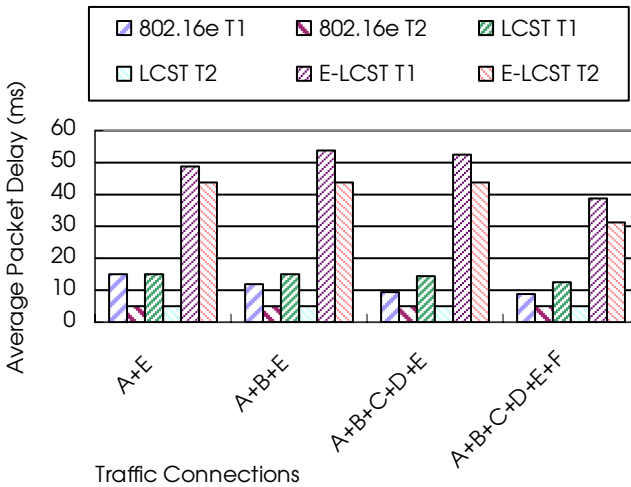


Fig. 12. The effect of number of type II connections on average packet delay

The listening windows of type II connections can transmit the MAC SDUs (service data units). If the size of a type II packet is smaller, the unused space in the listening window will be larger. In this situation, we can have higher probability to transmit type I packets within the type II listening window. Then the MSS will have more frames to enter the sleep mode. In Fig. 11, it shows the effect of packet size on the percentage of sleep periods. The A+E and C+E have more sleep periods than the A+G and C+G, respectively, because the packet size in connection E is smaller than that in connection G. The A+E also have a higher percentage of sleep periods than the C+E, because the packet size of A is smaller than that of C.

Note that the proposed two schemes were designed to piggyback the type I connection’s traffic indication message at the type II connection’s traffic indication message. If the number of type II connections is much less than type I connections, the percentage of sleep windows of our schemes will become smaller and the average

delay may become longer. In the following, we will evaluate this situation. In Fig. 12, there is only one type II connection E in the following cases: A+E, A+B+E and A+B+C+D+E. The average packet delay increases when the number of type I connections increases. This is because the total size of buffered packets is larger than the unused space that a listening window of type II can provide. The BS then has to transmit the unsent packets with another frame(s) and the packet delay becomes longer. In the case of A+B+C+D+E+F, there are two type II connections of equal packet size. Comparing between A+B+C+D+E and A+B+C+D+E+F, the average packet delay of the latter is smaller than the former, since the latter has more type II connections of equal packet size. Therefore, the proposed two schemes are suited to environments that allow type II connections to utilize its unused space in a frame to carry type I's packets.

5 Implementation Considerations

To implement the proposed method on an IEEE 802.16e system, firmware or embedded software for MSSs and BSs needs to be enhanced. Fig. 13 depicts a possible implementation of the proposed method on an IEEE 802.16e MSS SoC (System on Chip), and an IEEE 802.16e BS. The physical layer (PHY) and some time-critical MAC functions such as generating MAC header and packet encryption and integrity check are implemented in an ASIC chip. Management functions and high level MAC functions such as sleep mode operations are implemented in the embedded software or firmware depending on the architecture of the SoC. These functions control the SoC through an MAC driver. For the implementation of an MSS, the initial parameters of the sleep mode operation should be proposed by the LCST/E-LCST scheduler that sends a sleep mode request to the BS. The LCST or E-LCST scheduler on the BS which received the request must perform the admission control based on the sleep mode response from the MSS and finally responds the request. The final sleep mode schedule is determined by the BS, and the parameters of the sleep mode operations derived by the LCST/E-LCST scheduling algorithm on both the MSS and BS must be synchronized. While an MSS has a packet to send, the packet scheduler on the MSS checks the LCST/E-LCST scheduler to determine the

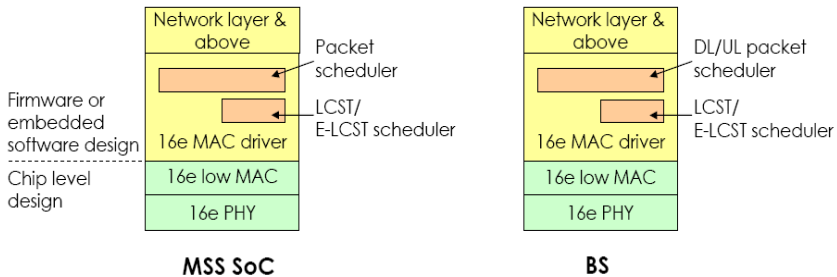


Fig. 13. Implementation of the proposed method on IEEE 802.16e SoC

transmission slots so that the packet scheduler can transmit the packets in the minimal number of frames. On the other hand, if the BS has packets to send to the MSS, it also checks the LCST/E-LCST scheduler on the BS and schedules the packets.

6 Conclusions

We presented two efficient energy saving schemes for the sleep mode operations in IEEE 802.16e. The proposed schemes can minimize the listening windows of power saving classes of non-real-time packets (type I) and schedule real-time packets (type II) in less number of frames. The main idea of the proposed schemes is to reduce the number of listening windows for transmitting/receiving packets from all service connections, so that there is more common sleep time for the MSSs to enter the sleep mode and save more power. According to the simulation results, the LCST and E-LCST performed 14% to 50 % and 33% to 68% better than the IEEE 802.16e scheme, respectively, in terms of percentage of sleep periods. However, more packet delay is introduced by the proposed schemes. The LCST and E-LCST introduced 6% to 77% and 84% to 88% longer average packet delay for non-real-time packets than the IEEE 802.16e scheme, respectively. Nevertheless, the delay of each type II connection still met its delay constraint. In other words, the QoS requirements of type II connections in our proposed two schemes were still met. The proposed schemes are compatible with the conventional IEEE 802.16e standard, because we only need to adjust the parameter values of sleep mode operations of types I and II in the base station.

References

1. IEEE 802.16-2004, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, Standard for Local and Metropolitan Area Networks (October 2004)
2. IEEE 802.16e-2006, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands (February 2006)
3. Xiao, Y.: Energy saving mechanism in the IEEE 802.16e wireless MAN. *IEEE Communication Letters* 9(7), 595–597 (2005)
4. Xiao, Y.: Performance analysis of an energy saving mechanism in the IEEE 802.16e wireless MAN. *Proceeding of IEEE CCNC 2006* 1(8-10), 406–410 (2006)
5. Seo, J.-B., Lee, S.-Q., Park, N.-H., Lee, H.-W., Cho, C.-H.: Performance analysis of sleep mode operation in IEEE 802.16e. In: *Proc. VTC2004-Fall*, vol. 2, pp. 1169–1173 (2004)
6. Chen, Y.-L., Tsao, S.-L.: Energy-Efficient Sleep-Mode Operations for Broadband Wireless Access Systems. In: *Proc. VTC 2006-Fall*, pp. 1–5 (2006)

Enhanced Fingerprint-Based Location Estimation System in Wireless LAN Environment*

Wilson M. Yeung, JunYang Zhou, and Joseph K. Ng

Department of Computer Science
Hong Kong Baptist University
Kowloon Tong, Hong Kong
{wilson, jyzhou, jng}@comp.hkbu.edu.hk

Abstract. Received Signal Strength (RSS) is one of the most useful information used for location estimation in Wireless LAN (WLAN). Most of the proposed WLAN positioning systems obtain RSS from either the Access Point or from the Mobile Device, but there are few researches that make use of the RSS obtained from both Access Points and Mobile Devices to perform location estimation. In this paper, we propose a new WLAN positioning system which makes use of the RSS collected from both the Access Points and Mobile Device. Our experimental result shows that the performance of our system is enhanced more than 23%, as compares to the traditional fingerprint-based WLAN positioning system which uses either RSS information obtained at Access Points or Mobile Device exclusively.

Keywords: Wireless LAN, Positioning, Location Estimation, Ubiquitous Computing.

1 Introduction

Mobile and wireless communication have become a crucial part of our daily life, thanks to the growth of the mobile and wireless technologies. As the cost of computing device decreases, many people own one or more computing devices for various usages, such as personal communication, office works, and entertainment. The advance in technologies and their applications have make Ubiquitous Computing possible and makes Ubiquitous Computing the new era of Computing. In particular, user's location is an important information for ubiquitous computing, as it enables location-aware services and therefore makes ubiquitous computing more practical and useful for daily life. That's why we need to explore, investigate and enhance positioning technologies for facilitating ubiquitous computing. Nowadays, we can easily obtain our location coordinates by the Global Positioning System (GPS). However, we can only receive GPS services in outdoor environment, as the GPS devices rely on signals from the satellite system surrounding the globe. Therefore many indoor positioning solutions [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#) based on radio frequency (RF) has been proposed in recent years. Among these previous works, Wi-Fi (IEEE 802.11) positioning become a hot topic for indoor positioning,

* This work is supported by the RGC Central Allocation from the Hong Kong SAR Government under the grant no. HKBU 1/05C.

as Wireless LAN (WLAN) has become a basic infrastructure of many buildings. Many WLAN positioning systems have been proposed in the literature, and most of them use Received Signal Strength (RSS) as input data for location estimation. However, previous works mainly focused on using the RSS obtained either at Access Point (AP) or the Mobile Device (MD). In other words, there are few researches that use RSS obtained from both AP and MD as input data for location estimation. In fact, the signal strength of the signal transmitted from the AP to MD (downlink) and the signal transmitted from MD to AP (uplink) can be different, this is true even both AP and MD have the same level of transmission power [5], i.e. asymmetrical signal strength [5] [6]. Therefore, we can actually treat the uplink and downlink RSS as two different source of information for location estimation.

In this paper, we present a new WLAN positioning system, which use both uplink and downlink RSS as input data to locate the user. Similar to the RADAR system by Bahl et. al [7] [8], our system is based on location fingerprint to perform location estimation. Experimental results had shown that our system can provide a more accurate location, as compares to the system using either uplink or downlink RSS exclusively.

The rest of the paper is organized as follows. In Section 2 we introduce the related works. Section 3 presents our system. In Section 4 we describe our test site and the experiment setup, and present the experiment results and performance evaluation. And finally, in Section 5 we provide a summary of our study and research findings.

2 Related Work

There are many related works on WLAN by using RSS for estimating a user's location. The RADAR system by Bahl et. al. [7] [8] is a well known WLAN positioning system, which is a location fingerprint system. The sampling process of this system is using a mobile device (laptop computer) to broadcast packets and then measure the signal strength at the access points (Pentium-based PCs), i.e. the uplink approach. The RSS values from different access points are then gathered to form a RSS tuple. Besides the RADAR system [7] [8], other fingerprint-based [9] [10] system are also proposed, where these systems use the downlink approach to sample a RSS tuple. The basic idea of a location fingerprint system is to find out the nearest neighbor in the signal space [8] [7] [11] [9] [10] by calculating the distance (usually, the Euclidean distance) between the location of fingerprints recorded in the system and the RSS tuples obtained in real-time. In order to create location fingerprints, the sampling process must be taken at different pre-defined location, and hence a group of RSS tuples is collected at each of these known locations. Each group of RSS tuples is then used to build a location fingerprint (Say, by taking average value of RSS from each of the access points, i.e. the RADAR approach [7] [8]). These location fingerprints are then saved into the database of the location estimation system. Later on, in the locating phase, real-time or online RSS tuples at unknown location will be obtained, and the location that matches the closest RSS tuple (i.e. the location fingerprint) stored in the database will be the user's location.

Besides location fingerprint system, there is probability-based system which uses another way to handle the RSS samples. Basically, the probability-based system uses the

RSS samples to create probability distributions of signal strength for known locations. When a RSS tuple is obtained in real-time, it is matched to these probability distributions to find out the location with the highest probability. The HORUS system by Youssef et al. [12] [13] [14] [15], and the system by Xiang et al. [16] are probability-based WLAN positioning system, and both systems use the downlink approach to obtain the RSS tuples.

In fact, a few commercial products for Wi-Fi positioning can be found. Ekahau [17] performs positioning by collecting the RSS samples at the mobile device to build radio maps. And Cisco [18] states that their location tracking system measures the signal strength from the mobile device at the access points.

Rather than Wi-Fi base system, some other RF-based positioning systems [2] [3] [1] [4] have been proposed. MoteTrack system by Lorincz et al. [2] is one of the RF-based positioning systems. It uses a numbers of wireless sensor nodes, i.e. "Mote", to build a sensor network and to determine user's location by using the RSS information. In fact, many RF-based positioning systems used wireless node as a sensor. These nodes send and receive beacon packets and therefore obtain the RSS information. By gathering the RSS data from all these nodes, the location of a mobile node can be estimated. In this kind of sensor network environment, both the uplink and downlink RSS of a mobile node can be retrieved.

Previous work on WLAN positioning has mainly focused on using the RSS samples either collected at AP or MD, but not using RSS samples obtained from both side. Ganu et al. [5] has investigated and reported the existance and the characteristic of asymmetrical signal strength. However, no positioning approach based on asymmetrical signal strength is proposed in their studies. In our previous research [6], we proposed a positioning model based on asymmetrical signal strength and make use of both uplink and downlink RSS information. Since results are promising, this work is a further enhancement of our previous work as reported in [6].

3 Proposed System

Different from most of the previous works, our system considered the existance of asymmetrical signal strength, and therefore we used both uplink and downlink RSS as input data for location estimation.

3.1 Asymmetrical Signal Strength

Theoretically, the received signal strength (RSS) should be proportional to the transmission power of transmitter. Supposes the distance between the transmitter and receiver is fixed, then the RSS value measured at receiver should be higher if we increase the output power of the transmission; or the RSS value should be lower if the transmission power is reduced. However, Ganu et al. [5] have shown that even the AP and MD has the same level of transmission power, the downlink and uplink RSS value measured at the AP and MD can be different due to different design [5]. In fact, the transmission power of the AP and MD are seldom at the same level, due to some practical reasons. For an example, the AP needs to cover a larger area and therefore it needs higher transmission power; On the other hand, the MD needs to save the battery power and usually

the transmission power is much smaller as compared to the AP [6]. As long as asymmetrical signal strength exists, our proposed system has considered and made use of this characteristic to enhance the performance of the location estimation system.

3.2 Methodology

In our proposed system, we have two sets of training data: $\{s_i^{(d)}\}$ and $\{s_i^{(u)}\}$, which represent two sets of RSS data collected at some known location l_i by the downlink, and uplink approach, respectively, in the offline (training) phase. Meanwhile, two observed RSS tuples, s_a and s_b , are obtained at a unknown location θ by the downlink, and uplink approach, respectively, in the online phase. $s_i^{(d)}, s_i^{(u)}, s_a$ and s_b are $m \times 1$ vectors, where m is the number of access points. By combining two downlink and uplink data source, we have a training data source: $\{\{s_i^{(d)}\}, \{s_i^{(u)}\}, l_i\}_{i=1}^n$, where n is the number of sample points. Our proposed system is to find out the unknown location θ based on (s_a, s_b) , obtained in real-time, and the training data source. And hence, we need a metric to pick up the one that best matches the observed signal strength.

Euclidean distance is a common measurement to describe the distance between two points in free space, which is widely used in real application. Mahalanobis distance can be thought of as an extension to the Euclidean distance, which takes into account the correlations of the data set. In fact, Mahalanobis distance is widely used in cluster analysis and other classification techniques. The composed distance is a metric to describe the distance between two points based on the merged data source, while the metric of probability is based on the Maximum Likelihood rule. We assume that the received signals follow a multiple normal distribution, then we choose the one that maximizes the probability as the solution.

We describe these criteria in detail as follows:

Euclidean Distance. The idea of Euclidean Distance is to compute the distance between the observed RSS tuple, $s = (s_1, s_2, \dots, s_m)^T$, and the mean RSS tuple, $\overline{s^*} = (\overline{s_1^*}, \overline{s_2^*}, \dots, \overline{s_m^*})^T$. The distance is defined as:

$$d = \sqrt{(s - \overline{s^*})^T (s - \overline{s^*})} \tag{1}$$

Then

$$\begin{cases} da_i = \sqrt{(s_a - \overline{s_i^{(d)}})^T (s_a - \overline{s_i^{(d)}})}, & \text{downlink} \\ db_i = \sqrt{(s_b - \overline{s_i^{(u)}})^T (s_b - \overline{s_i^{(u)}})}, & \text{uplink} \end{cases} \tag{2}$$

where $\overline{s_i^{(d)}}$ and $\overline{s_i^{(u)}}$ are the mean of the recorded RSS at point i from downlink and uplink respectively.

The result location is the one that minimizes da_i or db_i , as the RADAR [7] [8] does, i.e.:

$$\theta = \{l_i : da_i = \min\{da_j, j = 1, \dots, n\} \text{ or } db_i = \min\{db_j, j = 1, \dots, n\}\}$$

Mahalanobis Distance. Mahalanobis distance differs from Euclidean distance in that it takes into account the correlations of the data set.

Formally, Mahalanobis distance is defined as:

$$md = \sqrt{(s_a - \overline{s^*})^T (\Sigma^*)^{-1} (s_a - \overline{s^*})} \quad (3)$$

Then we have,

$$\begin{cases} mda_i = \sqrt{(s_a - \overline{s_i^{(d)}})^T (\Sigma_i^{(d)})^{-1} (s_a - \overline{s_i^{(d)}})}, & \text{downlink} \\ mdb_i = \sqrt{(s_b - \overline{s_i^{(u)}})^T (\Sigma_i^{(u)})^{-1} (s_b - \overline{s_i^{(u)}})}, & \text{uplink} \end{cases} \quad (4)$$

where $\overline{s_i^{(d)}}$ and $\overline{s_i^{(u)}}$ are the mean of the recorded RSS and $\Sigma_i^{(d)}$ and $\Sigma_i^{(u)}$ are the covariance of the recorded RSS at point i from downlink, and uplink respectively.

Suppose $\{s_{ij}^{(d)}\}_{j=1}^m$ and $\{s_{ij}^{(u)}\}_{j=1}^m$ are the signals received from downlink and uplink in location l_i , then $\overline{s_i^{(d)}}$, $\overline{s_i^{(u)}}$, $\Sigma_i^{(d)}$ and $\Sigma_i^{(u)}$ are defined as:

$$\begin{cases} \overline{s_i^{(d)}} = \frac{1}{m} \sum_{j=1}^m s_{ij}^{(d)}, & \text{downlink} \\ \overline{s_i^{(u)}} = \frac{1}{m} \sum_{j=1}^m s_{ij}^{(u)}, & \text{uplink} \end{cases} \quad (5)$$

$$\begin{cases} \Sigma_i^{(d)} = \frac{1}{m} \sum_{j=1}^m (s_{ij}^{(d)} - \overline{s_i^{(d)}})(s_{ij}^{(d)} - \overline{s_i^{(d)}})^T, & \text{downlink} \\ \Sigma_i^{(u)} = \frac{1}{m} \sum_{j=1}^m (s_{ij}^{(u)} - \overline{s_i^{(u)}})(s_{ij}^{(u)} - \overline{s_i^{(u)}})^T, & \text{uplink} \end{cases} \quad (6)$$

where $\Sigma_i^{(d)}$ and $\Sigma_i^{(u)}$ describe the covariance of the downlink data and uplink data.

The solution, i.e. the estimated location, is the location i has the minimum value of mda_i or mdb_i , that is:

$$\theta = \{l_i : mda_i = \min\{mda_j, j = 1, \dots, n\} \text{ or } mdb_i = \min\{mdb_j, j = 1, \dots, n\}\}$$

Composed Distance. We have the downlink data and the uplink data, and we want to combine these two sets of data to find out a criteria to choose the best solution. One intuitive idea is the one that composes da_i and db_i , where da_i and db_i are defined by eq. (2), i.e. $d_i = da_i \times db_i$, which is a metric defined in the merge data space. The solution is the location that has the minimum d_i . Namely,

$$\theta = \{l_i : d_i = \min\{d_j, j = 1, \dots, n\}\}$$

Probability. Assuming s_a and s_b follow multiple normal distributions and they are independent, then we have:

$$prob(s_a|l) = \frac{1}{(2\pi)^{m/2} |\Sigma^{(d)}|^{1/2}} \exp\left(-\frac{(s_a - \overline{s^{(d)}})^T (\Sigma^{(d)})^{-1} (s_a - \overline{s^{(d)}})}{2}\right) \quad (7)$$

where $\overline{s^{(d)}}$ is the mean of the recorded RSS and $\Sigma^{(d)}$ is the covariance at location l from the downlink data. Similarly, we can apply the same formula on the uplink data, i.e.

$$prob(s_b|l) = \frac{1}{(2\pi)^{m/2}|\Sigma^{(u)}|^{1/2}} \exp\left(-\frac{(s_b - \overline{s^{(u)}})^T(\Sigma^{(u)})^{-1}(s_b - \overline{s^{(u)}})}{2}\right) \quad (8)$$

where $\overline{s^{(u)}}$ is the mean and $\Sigma^{(u)}$ is the covariance at location l from the uplink data.

We define a likelihood function with s_a and s_b based on location l_i :

$$prob(s_a, s_b|l_i) = prob(s_a|l_i)prob(s_b|l_i) \quad (9)$$

That is,

$$prob(s_a, s_b|l_i) = \frac{1}{c} \exp\left(-\frac{(s_a - \overline{s_i^{(d)}})^T(\Sigma_i^{(d)})^{-1}(s_a - \overline{s_i^{(d)}}) + (s_b - \overline{s_i^{(u)}})^T(\Sigma_i^{(u)})^{-1}(s_b - \overline{s_i^{(u)}})}{2}\right) \quad (10)$$

where $c = (2\pi)^m \cdot |\Sigma_i^{(d)}|^{1/2} \cdot |\Sigma_i^{(u)}|^{1/2}$ is independent with s_a and s_b , and it depends on l_i .

The solution is the location whose $\overline{s_i^{(u)}}$ and $\overline{s_i^{(d)}}$ can maximizes the likelihood function, which is the Maximum Likelihood Estimator (MLE).

We set

$$\begin{cases} mda_i^2 = (s_a - \overline{s_i^{(d)}})^T(\Sigma_i^{(d)})^{-1}(s_a - \overline{s_i^{(d)}}), & \text{downlink} \\ mdb_i^2 = (s_b - \overline{s_i^{(u)}})^T(\Sigma_i^{(u)})^{-1}(s_b - \overline{s_i^{(u)}}), & \text{uplink} \end{cases} \quad (11)$$

Therefore the likelihood function can be rewritten as:

$$prob(s_a, s_b|l_i) = \frac{1}{(2\pi)^m \cdot |\Sigma_i^{(d)}|^{1/2} \cdot |\Sigma_i^{(u)}|^{1/2}} \exp\left(-\frac{mda_i^2 + mdb_i^2}{2}\right) \quad (12)$$

Then the solution is

$$\theta = \{l_i : prob(s_a, s_b|l_i) = \max\{prob(s_a, s_b|l_j), j = 1, \dots, n\}\}$$

In our system, we implemented both the "Composed Distance" and the "Probability" approaches, since they can make use of both the uplink and downlink RSS data simultaneously. We will compare these results with the RADAR system and the one with Mahalanobis distance and investigate how much performance gain can be obtained by utilizing both the uplink and downlink RSS data for location estimation.

4 Performance

In this section, we present the experiment setup for testing our proposed system, the experimental result and analysis for our study.

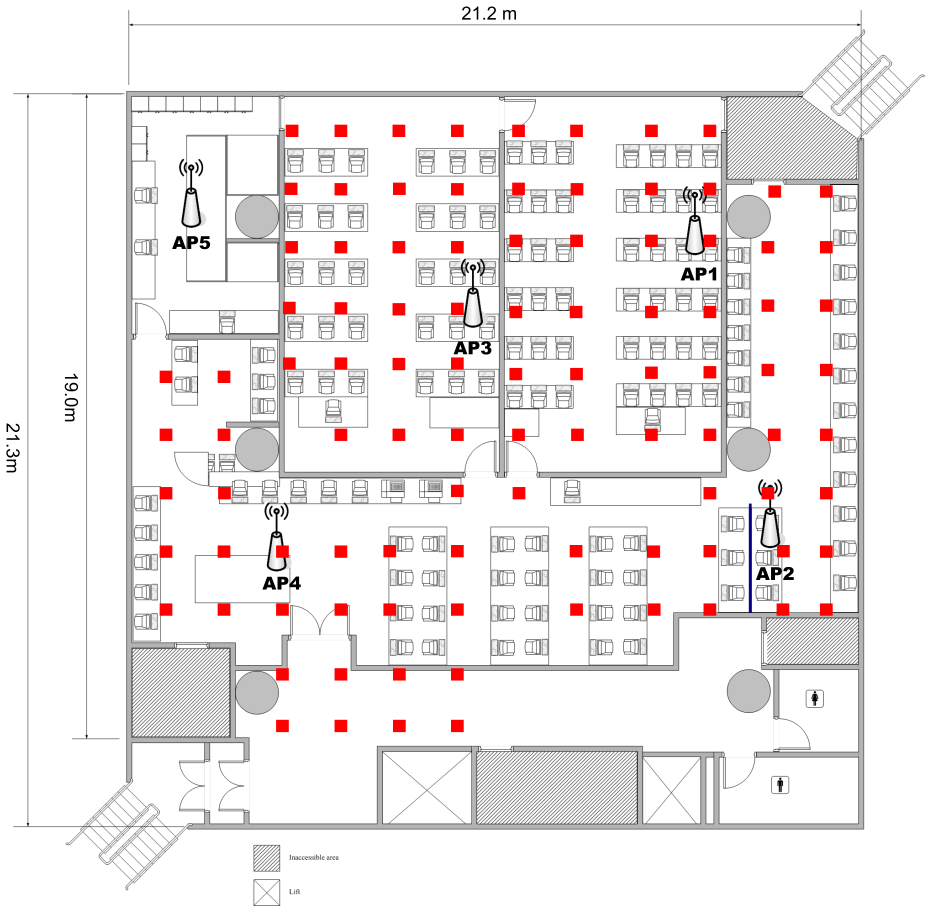


Fig. 1. The testbed for our experiment with 5 APs, where the red squares indicate the sampling locations

4.1 Experiment Setup

Testbed for the experiment. Our experiments were performed on the third floor of a six-storey building, which is a computer laboratory of the Computer Science Department at HKBU. Figure 1 shows the floor plan of the lab and the dimension of the testbed are 21.3m by 21.2m, covering an area of 451.56 m².

In the testbed, five access points are installed. We used an open source wireless router (Linksys WRT54GL [19]) as our access point. Besides, we installed OpenWRT [20] to replace the original software that bundled with the router. OpenWRT is an open source Linux distribution, which allows us to have more control in sending and receiving signals to and from the mobile devices. To obtain RSS of the mobile device at the access point, we used a self-developed tool, which run on the access point, to grab the packets from the mobile device, and hence getting the RSS. All the RSS records were then sent

to and stored in our database server. For the mobile device, we used the HP iPAQ 4150 Pocket PC, which has a built-in 802.11b wireless LAN card. We also developed another tool which runs on the Pocket PC in order to obtain the RSS sample at the mobile device. This tool can report the RSS from each access point by calling the system API to perform an active scan.

Data Collection. In the experiment, we identified 99 sampling locations in the public area of the testbed, marked as red square in floor plan of Figure 1. Each sampling location is about 1.8m apart from the neighbor sampling locations. The area covered by the sampling location is about $305.5m^2$. All sampling locations were covered by all 5 access points.

We collected RSS sample in each of the 4 directions (north, east, south and west), and we collect 50 samples for each direction. We collected two sets of RSS samples, i.e. one set collected at the access point (uplink approach) and another set at the mobile device (downlink approach). Each set of data contains 19,800 RSS samples. We used 80% of the samples as training data for training, and the rest of the 20% of the samples were used for testing. In each iteration of the test, we randomly selected one test sample from both sets of testing data, where both test samples are collected at same known location.

Performance Studies. In our experiments, we want to evaluate 1) the performance of a positioning system similar to RADAR system but using Mahalanobis Distance to replace Euclidean Distance(RADAR system uses Euclidean Distance) on either uplink or downlink data(we use "System MD" to denote this system for the rest of the paper); 2) the performance of the system which applied "Composed Distance" or "Probability" methods where these methods use both uplink and downlink data. 3) The performance comparison between RADAR and our system, actually this is the comparison between using either uplink or downlink data and using both data.

4.2 Experimental Results and Analysis

Figure 2, 3 & 4 show the the cumulative distribution function (CDF) of the error distance among different systems. From figure 2, we can observe that the accuracy of RADAR system and System MD are more or less the same when they were applied with the downlink data. System MD yielded better performance at 30% but it's worse than RADAR system at 85% of cumulatively probability. However, when the uplink data is applied, the two systems obtain different performance. Figure 3 shows that the the RADAR system performed better than System MD in most of the time. It is because the uplink signal is transmitted from MD to AP, and the transmission power of MD is smaller. If background noise in the testbed is constant, then uplink channel should has lower Signal to Noise Ratio (SNR), and therefore the uplink data should be more noisier than the downlink data. By comparing the experimental results of uplink and downlink data, we think that System MD is more sensitive to signal noise. The performance of our proposed system with "Composed Distance" and "Probability" are shown in figure 4. In most of the time, the performance of these two approaches are the same, except the significant difference at 40% of cumulative probability. Among

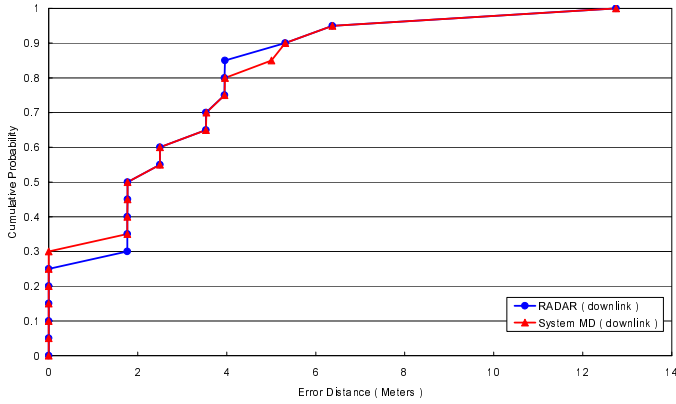


Fig. 2. Cumulative error distance of uplink data

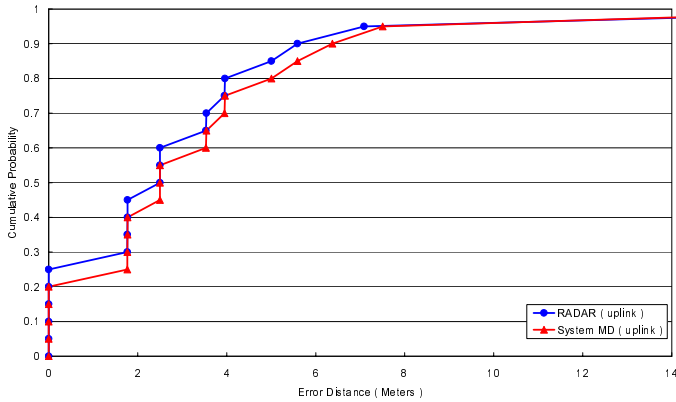


Fig. 3. Cumulative error distance of downlink data

Table 1. Performance Summary

| | RADAR | | System MD | | Our System | |
|---|----------|--------|-----------|--------|--------------------------|--------------------|
| | Downlink | Uplink | Downlink | Uplink | Mix(Composed Distance) | Mix(Probability) |
| Average (m) | 2.47 | 2.65 | 2.42 | 2.97 | 1.88 | 1.78 |
| Std. Dev.(m) | 2.14 | 2.47 | 2.22 | 2.58 | 1.95 | 1.93 |
| Max(m) | 12.75 | 21.30 | 12.75 | 20.16 | 18.81 | 13.82 |
| Min(m) | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| 90% Percentile(m) | 5.31 | 5.59 | 5.31 | 6.37 | 3.96 | 3.96 |
| Confidence Interval($\alpha = 0.05$)(m) | 0.039 | 0.045 | 0.041 | 0.047 | 0.036 | 0.035 |

these figures, we can observe that the RADAR system and System MD perform better when they were applied with uplink data, as compared with result of the downlink data.

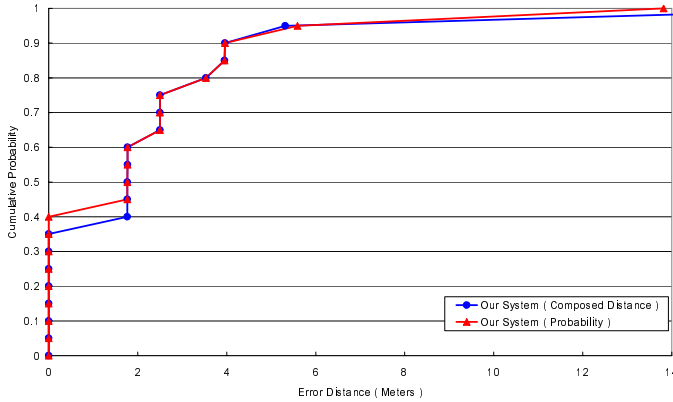


Fig. 4. Cumulative error distance of our system

Table 2. Enhancement in percentage

| | Our System | |
|------------------|-----------------------------|-----------------------|
| | Composed Distance Technique | Probability Technique |
| RADAR (downlink) | 23.90% | 28.98% |
| RADAR (uplink) | 27.78% | 32.60% |

However, when both uplink and downlink data were applied, our proposed system performs better than systems using uplink data and, of course, the downlink data.

Table 1 summarized the performance of RADAR, System MD, and our proposed system. Our proposed system yielded a smaller average error distance over the other two systems. The average error distance of the system with "Composed Distance" method is $1.88m$ and, the system with the "Probability" method yield a slightly smaller value, i.e. $1.78m$. System MD with uplink RSS data obtained the largest value of average error distance, that is $2.97m$. The standard deviation of the error distance of the system with the "Probability" method is $1.93m$, which is the smallest value among all systems. However, when the RADAR system and System MD used with downlink data, both of them obtained the smallest value for the Maximum error distance, i.e. $12.75m$. Besides, the maximum error distance of the system with the "Probability" method is about $5m$ shorter than the system with the "Composed Distance" method. Finally, Table 2 shows the performance enhancement of our system over the RADAR system. The performance of our system has outperformed the RADAR system by 23.90% to 32.60%.

In the point of view of accuracy, "Probability" methods are more accurate than "Composed Distance" methods, but it demands a higher computation cost. On the other hand, "Composed Distance" methods perform nearly the same as "Probability" methods but with a lower computation cost. Therefore if we demand better accuracy, we should adopt the "Probability" methods, otherwise, for lower computation cost, one should adopt the "Composed Distance" method for a comparable accuracy.

5 Summary and Future Work

In this paper, we presented a WLAN positioning system which fully utilized the RSS collected from both the access points and mobile device. In our experiment, the accuracy of our system has improved for 23% to 32% over the traditional fingerprint-based positioning system.

Experimental results show that uplink data are noisy than the downlink data, and therefore the use of the uplink data may lower the performance of a positioning system. However, we can consider to apply other positioning algorithm, rather than location fingerprint algorithm, on the uplink data. In other words, we can actually apply two different positioning algorithms on downlink and uplink data, and this approach may further enhance the accuracy of user's position. We are going to investigate and evaluate this approach as our future work. In fact, if two different algorithms are applied, we may need a method to combine the results generated by the algorithms and, therefore, we will also investigate this kind of methods in our future research.

References

1. Ray, S., Starobinski, D., Trachtenberg, A., Ungrangsi, R.: Robust location detection with sensor networks
2. Lorincz, K., Welsh, M.: A robust, decentralized approach to rf-based location tracking. Technical Report TR-04-04, Harvard University (2004)
3. Ramadurai, V., Sichitiu, M.L.: Localization in wireless sensor networks: A probabilistic approach. In: ICWN 2003. Proceedings of the 2003 International Conference on Wireless Networks, pp. 275–281 (2003)
4. Vandebussche, K.: Fine-grained indoor localization using wireless sensor nodes. Master's thesis, Delft University of Technology (August 2005)
5. Ganu, S., Krishnakumar, A.S., Krishnan, P.: Infrastructure-based location estimation in wlan networks. In: WCNC 2004. Proceedings of the IEEE Wireless Communications and Networking Conference (2004)
6. Yeung, W.M., Ng, J.K.: Wireless LAN Positioning based on Received Signal Strength from Mobile device and Access Points. In: Proceedings of RTCSA (to appear 2007)
7. Bahl, P., Padmanabhan, V.N.: RADAR: An in-building RF-based user location and tracking system. *INFOCOM (2)*, 775–784 (2000)
8. Bahl, P., Balachandran, A., Padmanabhan, V.: Enhancements to the RADAR user location and tracking system. Technical report, Microsoft Corporation (February 2000)
9. Wong, W.H., Ng, J.K., Yeung, W.M.: Wireless lan positioning with mobile devices in a library environment. In: Proceedings of ICDCS-MDC 2005 Workshop, Columbus, Ohio, USA, pp. 633–636 (2005)
10. Yeung, W.M., Ng, J.K.: An Enhanced Wireless LAN Positioning Algorithm based on the Fingerprint Approach. In: Proceedings of IEEE TENCON 2006, Hong Kong, China (November 2006)
11. Cheng, Y., Chawathe, Y., LaMarca, A., Krumm, J.: Accuracy characterization for metropolitan-scale wi-fi localization (2005)
12. Youssef, M., Agrawala, A.: The horus wlan location determination system (June 2005)
13. Youssef, M., Agrawala, A., Shankar, U.: Wlan location determination via clustering and probability distributions (March 2003)

14. Youssef, M., Agrawala, A.: On the optimality of wlan location determination systems. Technical Report UMIACS-TR 2003-29 and CS-TR 4459, University of Maryland, College Park (March 2003)
15. Youssef, M.A., Agrawala, A., Shankar, A.U., Noh, S.H.: A probabilistic clustering-based indoor location determination system. Technical Report UMIACS-TR 2002-30 and CS-TR 4350, Department of Computer Science and UMIACS, University of Maryland (March 2002)
16. Xiang, Z., Song, S., Chen, J., Wang, H., Huang, J., Gao, X.: A wireless lan-based indoor positioning technology. IBM Journal of Research and Development 48 (2004)
17. Ekahau, Inc., <http://www.ekahau.com>
18. Cisco Systems, Inc.: Wi-fi based real-time location tracking: Solutions and technology (2006)
19. Cisco Systems, Inc.: Linksys WRT54GL V1.1 Wireless-G Broadband Router (2006), <http://www.linksys.com/>
20. OpenWRT: White Russian RC6 (2006), <http://openwrt.org/>

Improving Channel Scanning Procedures for WLAN Handoffs*

Shiao-Li Tsao and Ya-Lien Cheng

Department of Computer Science, National Chiao Tung University
sltsao@cs.nctu.edu.tw

Abstract. WLAN has been widely deployed over public and private areas and has become one of popular access technologies for mobile Internet services in recent several years. Handoff between WLAN access points (APs) that introduce packet loss and delay is one of the critical issues for mobile Internet applications, especially for real-time communications. Previous studies indicated that channel scanning time contributes a significant portion of handoff latency and introduces packet loss and delay. Therefore, solutions based on active scan were proposed to reduce total scanning time of channels so that the service disruption of a communication can be minimized. The other solutions based on passive scan scattering scans between packets did not optimize the total scanning time but avoid packet loss and delay. However, solutions for channel scanning procedures which combine active and passive scan strategies and take total scan latency, packet loss, and delay together into consideration have not yet been investigated. In this paper, a generic channel scanning model is proposed and solutions to improve scanning procedures for WLAN handoff are presented. Simulation results demonstrate that the proposed approaches achieve faster scan time than the existing solutions without violating packet delay and loss requirements specified by the applications during WLAN handoff. Moreover, the implementation of the proposed mechanisms on a WLAN SoC (System-on-Chip) is also discussed in this paper.

Keywords: WLAN, mobility management, channel scan, handoff.

1 Introduction

The development of the IEEE 802.11 standards offers new opportunities of wireless accesses for mobile communications, services and applications [1][2][3][4]. However, the coverage of a WLAN access point (AP) is normally 50 to 300 meters and the small WLAN coverage results in frequent handoffs between APs for moving users. A handoff that may disrupt a communication for hundreds of milliseconds to several seconds introduces serious packet delay and loss. The handoff latency significantly influences the qualities of communications, especially for real-time streaming applications and voice communications [3][9][10]. Hence, to minimize handoff delay becomes one of the most important research issues for WLANs.

* This work was supported by the NCTU-MediaTek Research Center under Grant Q583.

A WLAN handoff composes of three phases, i.e. scan phase, re-authentication phase and re-association phase. The scanning phase discovers the APs that an STA can hear and measures the signal strengths of these APs. It takes about several hundred milliseconds. The re-authentication phase verifies the access rights of an STA to a specific AP. Finally, the re-association phase negotiates with the target access point and re-establishes the connection [2]. For a WLAN without IEEE 802.1x and IEEE 802.11i security, previous studies have investigated that the scanning phase contributes up to 90% of the total handoff latency [5]. To scan WLAN channels in order to obtain signal strengths from APs before handoff, the IEEE 802.11 specification defines two scan strategies, i.e. passive scan and active scan [1][7]. For passive scan, a station (STA) scans a channel by switching to the channel and listening beacons from access points (APs) in the channel. Since an STA may not know the arrival time of beacons, the STA typically has to stay on the channel for a beacon interval, say 100ms, and waits for beacons. Generally speaking, the scan latency for passive scan strategy is determined by the length of beacon interval and usually introduces long channel scanning time. On the other hand, an STA can actively broadcast probe request messages to all APs on a channel, receives response messages from APs and then obtains their signal strengths. The channel scanning time for active scan is determined by the number of channels to scan, and the time to stay on a channel and wait for the responses message. Several studies have been worked on reducing the active scan time. For example, an STA can learn from the environment by the historical data or via pre-configurations [4][5] and then the STA uses the cache or neighbor information to eliminate the unnecessary scans on these channels without APs [8]. Although the total scanning time is reduced, they do not consider the service disruption for active connections. The service disruption is especially sensitive for real-time communications such as voice over IP and video streaming. Therefore, SyncScan was proposed by Ramani and Savage [6] based on the passive scan strategy. An STA can hear beacons from APs which are synchronized and broadcast beacons at the scheduled time intervals. Therefore, the STA only needs to switch to different channels at proper time and can obtain the signal strengths from APs through beacon messages. Without staying on the channel and waiting for probe response messages, this approach greatly reduces the packet loss and delay for real-time connections. However, this mechanism requires all APs to be synchronized and broadcast their beacons in a scheduled manner. Also, the total scanning time of the passive scan approach is longer than that of the active scan strategies because scans for all channels are not scheduled together but scattered between packet transmissions. The disadvantage of this approach is that the APs need to reconfigured and synchronized, and the approach might not be very practical for the existing WLAN infrastructures which have been already deployed. Moreover, it takes more time to scan all channels and the method cannot support urgent scan and handoff requests which need a fast scan results.

In this paper, a generic channel scanning model which combines active scan and passive scan strategies is proposed. We first present the optimal solution and then propose a heuristic algorithm to obtain fast and near-optimal results. The proposed

scan strategies not only consider packet delay and loss requirements specified by applications but also minimize the total channel scanning time. The rest of the paper is organized as follows. In Section 2, the problem is described. Section 3 presents the combined active and passive scan strategies, including the optimal solution and a heuristic algorithm. Performance evaluations and implementation of the proposed method on a WLAN SoC (System-on-Chip) are discussed in Section 4, and finally Section 5 concludes this work.

2 Problem Statements and Modeling

Consider that a WLAN hotspot has N WLAN APs which are denoted as AP_1, AP_2, \dots , and AP_N , they are deployed over C channels, i.e. CH_1, CH_2, \dots , and CH_C . Different from SyncScan [6] which requires extra management and configuration procedures on APs in order to synchronize APs and broadcast beacons in a scheduled manner, we assume no extra management procedures have been applied to the APs. In other words, APs are not synchronized and APs broadcast beacons based on their own schedules. Thus, if the length of beacon interval for AP_i is B_i and AP_i broadcasts its beacon at time T_i , its next beacon should be announced at $T_i + B_i$. We assume an STA has the information including the channels that each AP stays, the lengths of the beacon intervals and the beacon broadcasting time for all APs. The information can be pre-configured on STAs or maintained on a server where the STA can query. For STAs without pre-configurations, it can also learn and cache the information by listening different channels while it has no packet to send or receive.

For an STA that knows the beacon broadcasting time and applies passive scan strategies for channel scanning, it has to switch to different channels before the beacons are broadcasted. An STA has to spend T_{sw} to switch the channel and T_b for waiting the beacon. However, for two or more APs broadcast the beacon at a similar time window which is called a collision, the STA has to decide which beacon to receive first. For the other beacons which are collided, the STA has to wait for another beacon interval. Figure 1 gives an example that an STA applies a passive scan strategy for channel scanning. In Figure 1, there are five APs. There are AP#1, AP#2, AP#3, AP#4 and AP#5 which are configured on channel 1, 1, 6, 11, and 11. The STA initially stays on channel #1 so that it first receives beacon from AP#1. After receiving a beacon from AP#1, it stays in channel #1 and listens for AP#2. After completing channel scan on channel #1, it switches to channel #6 to listen beacon from AP#3. Finally, it switches to channel #11 and receives beacons from AP#4 and AP#5. On the other hand, STAs can also use active scan strategy for channel scanning procedures. For an STA which uses active scan, it only has to switch to a channel, sends probe request messages to the channel, and then waits for responses from all APs in the channel. According to the IEEE 802.11 specification, the STA has to stay on a channel with APs for a maximal channel time T_{max} which is a manageable parameter. Active scan needs not consider the beacon schedules and can be performed at any time. Figure 2 shows an example that an STA applies an active scan strategy

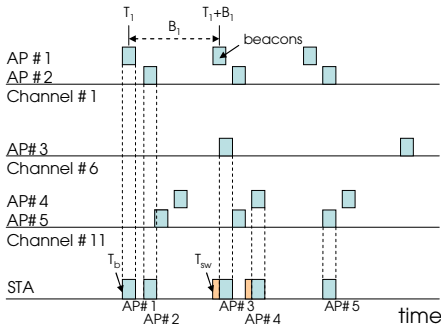


Fig. 1. Channel scanning based on the passive scan approach

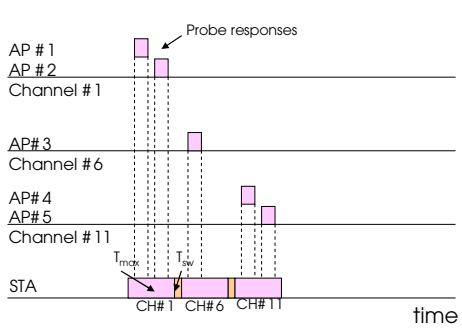


Fig. 2. Channel scanning based on the active scan approach

for channel scanning. The STA first scans channel #1, and then switch to the channel #6. After completing scan on channel #6, it switches to channel #11 and scans that channel.

If we further consider an STA currently has connections and has to perform the channel scanning procedures simultaneously, the packet transmission and receiving should be also considered together with the channel scanning schedule. For example, if there is a packet should be transmitted at a particular time and has been specified a maximal delay bound, the packet must be scheduled before its deadline. In other words, while an STA switch to a neighboring channel for an active or passive scan, it has to switch back to the serving channel and receives the packet before deadline. The channel scanning procedures should not influence QoS of the active connection, and this constraint is particularly important for these real-time connections such as voice over IP with QoS.

In this paper, a generic channel scanning problem is defined. Assume that an STA knows the AP and beacon information and has connections with QoS requirements. The QoS requirement here is the deadline for each packet. The STA uses both active and passive scan strategies for scheduling scanning procedures. The objective function of the scheduler on the STA is to optimize the total channel scanning time without violating packet delay requirements specified by the applications during WLAN handoff. Figure 3 shows an example where the STA uses the combined active and passive scan strategy to minimize the scan time and packet delay. In this example, AP#1 is the serving AP for an STA, and sends voice packets to the STA periodically. The STA knows the packet arrivals and has to switch back to the channel #1 in order to receive the packets from AP#1. The first example shows that the STA applies passive scan to scan the APs. The second example reveals that the STA uses active scan to scan the channels. The third example uses passive scan to scan AP#2, AP#4 and AP#5, and use active scan to scan channel #6. This example demonstrates that combined active and passive scan strategy may reduce the total scanning time. In the next section, an optimal solution for channel scanning and a heuristic algorithm are proposed.

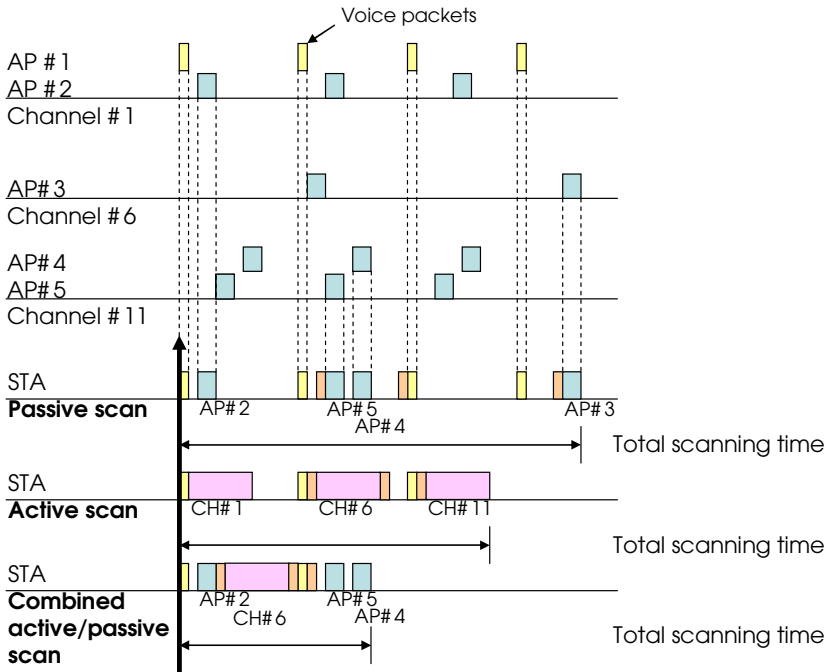


Fig. 3. Concurrent packet transmissions and channel scanning based on different channel scanning approaches

3 Optimal and Heuristic Algorithms

First, a scheduled list is defined. A scheduled list contains the scanning sequence and scanning time of all APs that the STA should follow. The starting time of the scheduled list should be the time that the STA wants to perform a channel scanning. The length of period that this scheduled list lasts for is called total scanning time. The total scanning time here is defined as the period between the start of the first scan and the complete of the last scan. In other words, an STA schedules the scanning procedures of APs or channels in the scheduled list and minimizes its length. The schedule policies are as follows. First, packets with delay constraints are scheduled. Second, the passive scan is then considered. The reason why we consider passive scan first is because beacon broadcasting time from APs are determined already. An STA has to follow APs' beacon broadcasting schedules if they want to receive their beacons. Third, active scan which can be performed at any time is finally scheduled. In order to meet the packet delay constraints specified by the application, these packets with delay constraints are first scheduled, i.e. inserted into the scheduled list, before channel scanning is scheduled. That is because we assume the QoS has a higher priority rather than channel scanning. For these applications that do not have delay constraints, packets do not have to insert into the list and the proposed model can be still used for these applications without packet delay requirements. For these

applications allows certain packet delays, the delay constraints will be also added into the scheduled list so that the scanning scheduler can adjust the packets to accommodate channel scheduling procedures without violating its delay requirement. After the packets are inserted, passive scan is then considered. Beacons from APs are then inserted into the scheduled list if there is no collision in the current list. The insertion function has to verify if the new inserted beacon is collided with the existing beacons or not. If the new beacon is collided, the two beacons and their next scheduled beacons will be marked in the scheduled list. That information helps the optimal algorithm to decide which beacon to scan or maybe an active scan is required.

3.1 The Optimal Algorithm

The optimal solution is to perform an exhausted search on all possible channel scanning sequences and to find the one with the minimal channel scanning time. Since active scan can be scheduled at any time, passive scan are scheduled first. After passive scan is scheduled, active scan are then insert and replace passive scan if the active scan can further reduce scanning time. Assume the scheduled list denotes a {AP#1, AP#2, AP #3 ..., AP #N}. The exhausted search on all possible combinations of passive scan can be derived. Through the number of APs increases, the number of possible solutions has exponential growth. To perform the exhausted search, dynamic programming technique has been applied. The previous results can be used to derive the new possible solutions. For example, only when AP#1 and AP#3 can be scheduled without collisions for passive scan, AP#1, AP#3 and AP#4 should be considered. Otherwise, it is no need to test if {AP#1, AP#3 and AP#4} is schedulable. The optimal algorithm by applying dynamic programming technique reduces the search cases.

After passive scan sequences have been derived, active scan for a specific channel can be inserted. If active scan is applied and the total scanning time can be reduced, APs in the same channel will be replaced by a channel number, say CH#M for example. That means the active scan will be applied to that channel instead of using passive scan. The optimal algorithm is described in Figure 4. Although the dynamic programming algorithm simplifies the solution-deriving process, it has a time complexity of $O(2^N)$. When there are too many APs to scan, it may become impractical due to the long scheduling time and the performance of the scanning phase will be seriously damaged. Thus, a heuristic algorithm is considered and proposed.

OPTIMAL()

Input: Lists of APs, their channel identifier and beacon broadcasting time.

Output: The scheduled list with the minimal channel scanning time

ScanTime: Minimal total scan time

TMPNode: (AP_{ID}, pTMPNode)

pTMPNode: pointer to the previous TMPNode

TMPList: temporary scheduled list


```

Create a new TMPNode, assign the channel identify as
NULL, and insert all APs to TMPList;

for APi
  for each TMPNodej in TMPList
    backup TMPNodej scheduled list
    insert APi into TMPNodej scheduled list
    if success then
      create a new newTMPNode
      copy TMPNode scheduled list to newTMPNode
      refer newTMPNode to TMPNodej, and insert
newTMPNode into TMPList
      Restore TMPNode scheduled list
    else
      Mark APi as scanned
    end if
  end for
end for
for TMPNodej in TMPList
  add active-scan for scanned AP
  calculate new ScanTime
end for
Return the best ScanTime;

```

Fig. 4. Optimal channel scanning algorithm

3.2 Heuristic Algorithm

To reduce the complexity to search all possible solutions, some APs which are not suitable for passive scan are removed from the passive scan search spaces. If only a part of APs is considered during passive scan schedules, the complexity can be considerably reduced. For example, for the channels have very few APs, they may be suitable for passive scan. Otherwise, if there are many APs in the same channel, active scan which can obtain all responses at one time should be applied to these channels. Therefore, we first screen the APs and remove these APs which are not suitable for passive scan. The test is basically to examine if the total passive scan time on these APs in the same channel exceeds the time for an active scan in that channel. After the procedure, the number of APs participating passive scan search is reduced.

After deciding the scanning type of each AP, an adjusting function is performed to further improve the scan time. The adjusting function checks the scheduled list and tries to replace the passive-scan slots of a channel with a single active scan slot to shorten the total turnaround time. Figure 5 presents the improvement of replacing the passive-scan slots of channel 4 with a single active scan slot. The adjusting function checks the time slots in the scheduled list from tail to head until the time slot checked cannot be replaced by any other earlier time slot. Through this mechanism, the resource utilization is improved during the scanning time while the delay constraints are satisfied. The total turnaround time is shortened as well. The detail heuristic algorithm is shown in Figure 6.

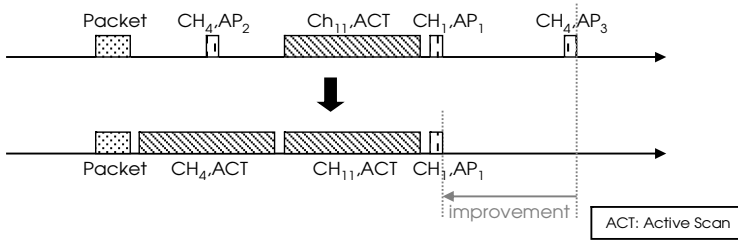


Fig. 5. Adjustment channel scheduling procedures

CANDIDATE()

Input: Lists of APs, their channel identifier and beacon broadcasting time.

Output: **CandiList:** candidate list of potential passive scan APs

```

for Channeli
    calculate Tact, which is the minimal active scanning
    time on APi under delay constraints
    calculate the passive scanning time for all AP in the
    channel
    if the passive scanning time is shorted than Tact
        insert AP in the channel i to CandiList and sort
        the list by the number of APs
    end for
Return CandiList
    
```

HEURISTIC ()

Input: Lists of APs, their channel identifier and beacon broadcasting time.

Output: The scheduled list with the minimal channel scanning time

ScanTime: Minimal total scan time

```

Call CANDIDATE() identify potential passive-scan APs
for APi in CandiList
    insert APi into scheduled list
    if failure
        mark APi as active scan
    end if
    remove redundant passive scan
    insert the active scan to scheduled list for these
APs marked as active scan
    call ADJUST to further improve the final schedule
    calculate ScanTime
end for
Return ScanTime;
    
```

Fig. 6. Heuristic algorithm

First, a candidate AP list where APs by applying passive scan may have a shorter scanning time than that by applying active scan is built. The APs in the candidate list will be sorted by the channel according to the number of APs on the same channel. The channels with less total passive scanning time are scheduled first. Then the channels in the candidates are checked one by one, until all of them are scheduled. The channels did not included into the candidate list, they should be scanned by using active scan. Since there may be more than one beacon slots from a single AP are inserted into the scheduled list, the algorithm checks the time slots and removes the redundancies. Then active-scan slots are inserted. After all channels are scheduled, the adjusting function is performed. The scheduled result is enhanced by the adjusting function to get better resource utilization and time performance. The heuristic solution has a time complexity of $O(N_b^2)$, where N_b is the number of beacons which are scheduled by using passive scan. The heuristic solution considerably reduces the time complexity compared with the optimal solution.

4 Simulation and Evaluation

In this section, simulations are conducted to evaluate the performance of the proposed approaches. The simulation program is written in C language, and four scanning mechanisms, including enhanced passive scan, enhanced active scan, optimal scan and the proposed heuristic mechanisms are implemented and evaluated. We assume the STAs know the information of all APs including the channel number, and beacon broadcasting time. The enhanced version passive and active scan mechanisms are denoted as ePAS and eACT which take advantages of the environment information to reduce the channel-waiting time. In the eACT mechanism, the STA always skips the channels without APs. In the ePAS mechanism, the STA knows the beacon arrival time of each AP and can hear the beacons exactly whenever they arrive to the channel. To simulate the WLAN network, one to ten APs are randomly generated and distributed over eleven channels. The beacon intervals for all APs are 100ms but they are not synchronized, i.e. the initial beacons for APs are different. Voice packets are sent to the STA every 20ms. For other WLAN parameters used in the simulations, they are the channel switching time ($T_{sw}=5ms$) [6], the maximal channel time ($T_{max}=11ms$), time to receive a beacon ($T_b=1ms$) [10]. Below evaluations are all based on the average results for 1000 time simulations which imply 1000 different channel configurations of WLAN APs are tested.

First, the delay constraint of voice packets is assumed 20ms and the total channel scanning time for the four different approaches is investigated. Figure 7 shows the simulation results. It can be seen from the figure while the number of AP increases, the average total scanning time also increases for all four approaches. For the eACT approach, it is because in our simulation, APs are randomly distributed to eleven WLAN channels. While the number of AP increases, the number of channels that have APs also increases. The eACT thus spends more time on average for the channel scanning. For the ePAS approach, the total scanning time increases faster than other three approaches while the number of AP increases. The reason is for a network with more APs, the STA has to spend more time to listen beacons from all APs passively. Moreover, more APs results in higher probability of beacon collisions than less APs.

To compare the performance between the ePAS, eACT and the proposed approaches, it can be found that when the number of AP is ten, the optimal solution, denoted as OPT, has the best performance of the average total scanning time which is 93.5 milliseconds. The proposed heuristic, denoted as HEU mechanism, achieves the second best result of 100.4 ms which is very close to the optimal solution. The optimal and heuristic solutions reduce 50% channeling scanning time than the ePAS. Also, the optimal and heuristic solutions can reduce 26% and 25% channel scanning time than eACT, respectively.

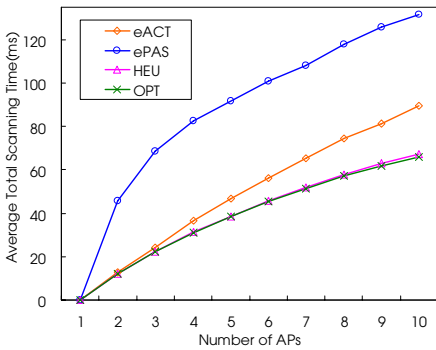


Fig. 7. Total scanning time for different scan mechanisms

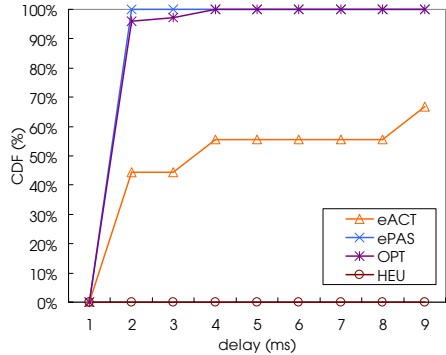


Fig. 8. Delay distribution of different mechanisms while the maximal delay is 20ms

Figure 8 shows the cumulative distribution of packet delay by applying different channel scanning mechanisms. In this simulation, only the extra delay due to channel scanning procedures is counted. The maximum delay of the voice packet due to channel scanning procedures is set to 20 ms for all four mechanisms in this simulation. It is important to note that if applications can tolerate more delay due to channel scanning procedures, the scanning time can be further reduced. The STA can schedule channel scanning first and then schedules packet transmission. Thus, the channel scanning time can be reduced. The channel scanning time and the maximum packet delay specified by applications are tradeoff. Figure 8 depicts the ePAS, the proposed optimal and heuristic method can all minimize packet delays. It can be seen that more than 90% of voice packets have less than one millisecond delay during handoff. ePAS is similar to SyncSCAN performs good in reducing packet delay during handoffs. Simulation results demonstrate that the proposed mechanisms outperform the eACT solution.

Finally, the execution time of heuristic and optimal channel scanning approach is compared. The two algorithms are run on a personal computer with AMD Athlon 1.83GHz CPU. The result is as shown in Figure 9. The execution time of the optimal solution increases exponentially while the number of total APs increases. When there are ten APs, the optimal solution needs 60ms to calculate the scanning schedule while

the heuristic approach merely needs 5ms. Although the optimal solution can also obtain the results fast, the computation overhead may not be acceptable if the optimal algorithm is executed in a mobile device which the computation power is much lower than a PC.

For most of WLAN chipsets or SoCs, the handoff policy is implemented in either firmware or software drivers. The chipsets and SoCs provide means such as control registers for software to control the scan procedures. For example, some WLAN chipsets or SoCs allow software to switch to a specific channel, send a specific message, and these functions can be integrated together to realize the proposed mechanisms. Similar to [6], the concept of proposed mechanisms can be implemented into the drivers. For these WLAN chipsets or SoCs which fully implement scan procedures using ASIC or does not provide control registers for software to change its scan behaviors, the implementation of the proposed mechanisms by using software is not possible. In that case, the modification of hardware is required.

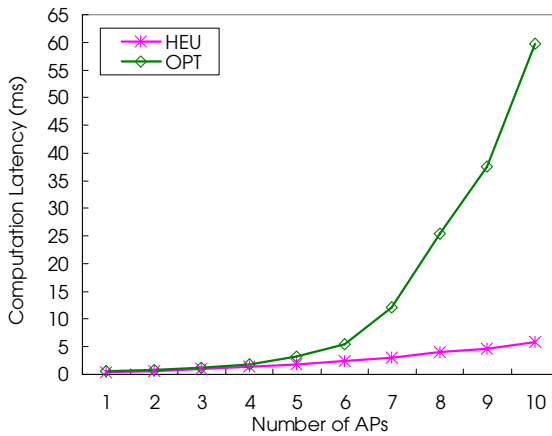


Fig. 9. Execution time for different mechanisms

5 Conclusions

In this paper, a generic channel scanning strategy which combines both active and passive scan mechanisms was presented. Based on the strategy, an optimal and a heuristic algorithm were proposed to minimize the total scanning time without violating the packet loss and delay requirements specified by the application during WLAN handoff. Simulation results demonstrate that about 30% to 50% scanning time can be reduced by applying the proposed algorithms while the QoS requirements can be also met. Comparing with optimal solution, the heuristic algorithm that significantly reduces the computation complexity can be easily implemented on mobile devices and achieves near-optimal results.

References

1. IEEE: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE standard 802.11 (1999)
2. IEEE: Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 2: Fast BSS Transition, P802.11r D1.0 (November 2005)
3. IEEE: Media Access Control (MAC) Enhancements for Quality of Service (QoS), IEEE Standard 802.11e (2006)
4. IEEE: Radio Resource Measurement Enhancements, IEEE 802.11k D1.0 (September 2004)
5. Mishra, A., Shin, M., Arbaugh, W.A.: An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process. *ACM SIGCOMM Comput. Commun. Rev.* 33(2), 93–102 (2003)
6. Ramani, I., Savage, S.: SyncScan: Practical Fast handoff for 802.11 Infrastructure Networks. In: *Proc. IEEE INFOCOM 2005* (March 2005)
7. Gast, M.S.: *802.11 Wireless Networks- The Definitive Guide*. O'REILLY (2005)
8. Shin, M., Mishra, A., Arbaugh, W.A.: Improving the Latency of 802.11 Hand-offs using Neighbor Graphs. In: *ACM MOBISYS 2004* (June 2004)
9. Markopoulou, A., Tobagi, F.A., Karam, M.J.: Assessment of VoIP quality over internet backbones. In: *IEEE INFOCOM 2002 - the Conference on Computer Communications* (June 2002)
10. Trad, A., Munir, F., Afifi, H.: Capacity Evaluation of VoIP in IEEE 802.11e Network Environment. In: *CCNC 2006. IEEE Consumer Communications and Networking Conference* (January 2006)

A Multicast Extension for Enhanced Mobile IP by Home Agent Handover

Chun-Chuan Yang¹, Jeng-Yueng Chen^{1,2}, and Li-Sheng Yu¹

¹ Department of Computer Science and Information Engineering,
National Chi Nan University, Puli, 545 Nantou, Taiwan

² Department of Information Management,
Hsiuping Institute of Technology, Dali, 412 Taichung, Taiwan
{ccyang, s2321902, s2321535}@ncnu.edu.tw

Abstract. In order to improve the routing efficiency and reduce handoff latency, we have proposed an enhancement of Mobile IP (MIP) called MIP with Home Agent Handover (HH-MIP) to enjoy most of the advantages of Route Optimization MIP (ROMIP) but with only a small increase of signaling overhead. In HH-MIP, the concept of Temporary Home Agent (THA) was proposed and the mobile host (MH) registers the new CoA with its THA rather than its original HA. In this paper, we propose a multicast extension for HH-MIP (HH-MIP/ME). HH-MIP/ME reduces routing inefficiency in bi-directional tunneling without generating large signaling overhead. Simulation results demonstrate that the proposed scheme enjoys small handoff latency as well as routing efficiency and the number of control packets generated in proposed scheme is significantly less than that in other approaches.

Keywords: Mobility, Multicast, Mobile IP, Route Optimization.

1 Introduction

Mobility management in the IP layer [1] is an essential component in wireless mobile networking. Mobile IP (MIP) [2]-[3] was proposed to support global Internet mobility through the introduction of location directories and address translation agents. In the MIP, a mobile host (MH) uses two IP addresses: a fixed home address and a care-of-address (CoA) that changes at each new point of attachment. A router called Home Agent (HA) on an MH's home network is responsible for maintaining the mapping (binding) of the home address to the CoA. When an MH moves to a foreign network, the MH obtains a CoA from the Foreign Agent (FA) and registers the CoA with its HA. In this way, whenever an MH is not attached to its home network, the HA gets all packets destined for the MH and arranges to deliver to the MH's current point of attachment by tunneling the packets to the MH's CoA. Some inefficiencies were identified in MIP: (1) Triangular routing from the sender (called correspondent node, CN) to the HA then to the mobile host leads to unnecessarily large end-to-end packet delay, (2) The HA is inevitably overloaded due to tunneling operations, and (3) When an MH is far away from its home network, the long signaling path for CoA registration leads to a long handoff latency resulting in a high packet loss. [4]-[5]

To remedy the problem of triangular routing and reduce the packet loss during handoff, Route Optimization MIP (ROMIP) [6]-[7] was proposed. The ROMIP allows every CN to cache and use binding copies. The original binding for an MH is kept in its HA, but the ROMIP supports that a binding copy can be propagated to the requiring nodes. Local bindings in a CN enable most packets in a traffic session to be delivered by direct routing. Moreover, an MH also informs its previous FA about the new CoA, so that the packets tunneled to the old location (due to an out-of-date binding copy) can be forwarded to the current location. This forwarding mechanism in ROMIP reduces the handoff latency and thus reduces the packet loss during handoff. However, the improvement of ROMIP over MIP in terms of routing efficiency and smaller handoff latency is at the cost of significantly larger signaling overhead.

An interesting point of view about the reason of the disadvantages of MIP in routing and handoff latency is because the MH has the potential to move away from its home network and the HA. If somehow we can dynamically make the HA closer to the current location of the MH, both routing and handoff efficiency can be achieved. Since the MH's home address is permanent, MH's HA should not move. Therefore, the idea of Temporary HA (THA) emerged and the extension of MIP adopting the THA called HA Handover MIP (HH-MIP) was proposed in [8]. The HH-MIP enjoys small handoff latency as well as routing efficiency and the number of control packets generated in the HH-MIP is significantly less than that in the ROMIP.

With the development of communication and multimedia technology, applications that use multicast as transmission method become more and more popular. However, the MIP is designated for unicast delivery to MHs. To perform multicast functionality, additional mechanisms must be added to the protocol to efficiently support multicast delivery within or on top of the MIP. The current version of the MIP proposes two approaches, called Remote Subscription (RS) and Bi-directional Tunneling (BT) [9], to support mobile multicast.

In the RS, the MH has to re-subscribe to its desired multicast groups while the MH moves to a new foreign network. This mechanism works well when the MH spends a relatively long time at each foreign network, compared with the join and graft latencies. The advantage of RS is it delivers multicast packets to related MHs in shortest path routes. However, RS introduces excessive control packets and packet loss because it needs to reconstruct multicast tree every time the MH moves to new foreign network.

With the BT, the MH sends and receives all multicast datagram from its HA. Multicast packets will be sent to the MH's HA and tunneled to current position of the MH using MIP unicast tunneling. This approach handles source mobility as well as recipient mobility, and in fact hides host mobility from all other members of the group. The main disadvantages of the protocol are the routing path for multicast delivery can be far from optimal (in the worst case, the source and the recipient can be on the same network, while all multicast messages between two hosts must traverse to the home agent before tunnel to the designated network) and the approach offers limited scalability. Some of the enhancement protocols based on bi-directional tunneling are Mobile Multicast (MoM) [10], Mobile Multicast Gateway (MMG) [11] and Range-base Mobile Multicast Protocol (RBMoM) [12].

In this paper, we introduce multicast extension based on our proposed mobility management protocol (HH-MIP) called HH-MIP Multicast Extension (HH-MIP/ME). Since the proposed multicast protocol is based on the HH-MIP, it will inherit the advantages of the HH-MIP. The proposed approach is a hybrid of RS and BT. We also use the idea developed from the MoM called Designated Multicast Service Provider (DMSP) [10]. The DMSP is used to solve the data duplication and tunnel convergence problem. The HH-MIP/ME reduces routing inefficiency in bi-directional tunneling without generating large signaling overhead. As will be shown in the simulation study, the HH-MIP/ME also enjoys small handoff latency as well as routing efficiency and the number of control packets generated in the HH-MIP is significantly less than that in the RS and BT-based MoM.

The rest of this paper is organized as follows. Section 2 reviews the HH-MIP approach. The proposed multicast extension of the HH-MIP is presented in section 3. Simulation studies for performance evaluation and comparison are presented in section 4. Finally, section 5 concludes this paper.

2 HH-MIP Approach

As mentioned in section 1, the HH-MIP introduces the concept of Temporary HA (THA) and as in the ROMIP each CN is required to maintain two addresses for an MH: the home address of the MH and the THA address of the MH. The HA of an MH maintains the binding of the THA address for the MH. Handover of the THA requires the MH to update the binding cache in its HA. The handoff of an MH to a new FA only triggers registration of the new CoA to the THA (instead of the HA) when the THA of the MH remains unchanged. Since the THA of an MH is selected to be close to the current location of the MH, the HH-MIP reduces the handoff latency and shortens the signaling path of registration as well.

Data delivery in the HH-MIP is similar to that in the ROMIP as explained in the following. Initially the CN sends packets to the home address of the destined MH, the HA intercepts and sends the packets to the THA by tunneling, and the THA tunnels the packets to the current location (FA) of the MH. Meanwhile, a binding copy of the MH's THA is sent by the HA to CN so that later packets can be directly delivered to the THA, and the THA tunnels the packets to the current location (FA) of the MH. Therefore, regular data delivery in the HH-MIP requires the packets sent by the CN to be tunneled twice before they reach the destined MH.

Four messages are used for binding update of THA as in ROMIP: (1) Binding Warning Message (M_W), (2) Binding Request Message (M_R), (3) Binding Update Message (M_U), and (4) Acknowledgement Message (M_A). The HA just after having tunneled the first packet sends an M_W back to the CN informing that the MH is not in the home network. In response to the received M_W , the CN sends an M_R to the HA asking for binding update. The HA replies with an M_U containing the requested CoA (i.e. THA's address). Finally, the CN sends an M_A to the HA acknowledging the successful binding update. Fig. 1 (a) illustrates the process of data delivery in the HH-MIP.

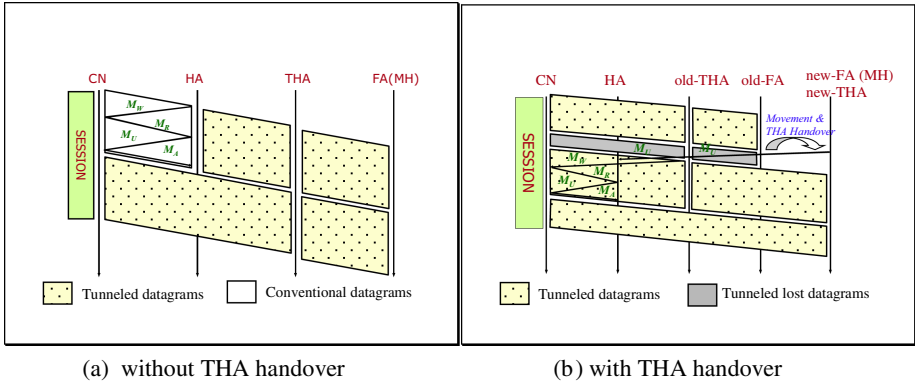


Fig. 1. Flow diagram for data delivery in HH-MIP

Initially, an MH will select its HA as the THA. The HH-MIP adopts an aggressive approach in selecting the THA for an MH: whenever an MH is moving away from the HA or the previous THA, the MH triggers the handover of THA. If the distance (hop count) from FA2 (MH's current location) to THA is longer than the distance from FA1 to THA implying that the MH is moving away from THA, FA2 is selected as the new THA, and the MH notifies its HA of the new THA. On the other hand, if HA is closer to FA2 than THA implying that the MH is moving back to HA, the HA should be selected as the new THA.

```

if Distance (FA2, HA) < Distance (FA2, THA) then
/** MH is moving closer to its HA ***/
  HA is selected as the new THA
else if Distance (FA2, THA) > Distance (FA1, THA)
/** MH is moving away from its previous THA ***/
  FA2 is selected as its new THA
else
  MH's THA remains the same
    
```

Once a new FA is selected as the new THA by an MH, the MH sends the Binding Update Message (M_U) to its HA as well as the previous THA. Before the CN gets the address of new THA (according to the M_U sent by the HA), packets are still tunneled to the previous THA (packets loss in this period), and the previous THA tunnels (forwards) the packets to the current FA (i.e. the new THA) which is similar to the forwarding mechanism in ROMIP. When the binding update of the new THA is complete in the CN, packets are sent directly to new THA. Flow diagram for the handover of THA is illustrated in Fig. 1 (b).

The HH-MIP adds new functional entity called Temporary Home Agent (THA) besides functional entities introduced in Mobile IP. Each FA or HA must be equipped with the functions of THA. The functions of the THA include: (1) maintaining a Temporary Children List (TCL) and dealing with the registration of the new CoA for every MH in the TCL, and (2) a previous THA for an MH is responsible for forwarding packets to the new THA after the MH performs THA handover.

HH-MIP also includes messages type that is similar to ROMIP. These messages include:

1. Binding Warning Message (M_W) - is sent to inform the target nodes about changing THA.
2. Binding Update Message (M_U) - is used to inform CN, old THA, or HA about the new THA address. THA can send M_U messages without waiting for request message.
3. Binding Request Message (M_R) - is sent by CN when it determines that its binding is stale and it wants to request connection to the THA.
4. Binding Acknowledge Message (M_A) - is used to acknowledge the reception of binding update message (M_U). Not every binding update need to be acknowledged.

3 Proposed HH-MIP/ME Approach

3.1 Basic Idea and Data Delivery

As we build our multicast extension on the top of HH-MIP, MH relies on THA to forward multicast traffic to MH through the tunneling via the FA. In this approach, THA will join multicast group on behalf of MH. As MH moves to other FA (without THA handover), multicast packets will be sent to THA and THA will tunnel the packets to MH's current position (FA). As illustrated in Fig. 2, THA will join multicast group on behalf of MH. Multicast Sender sends multicast packets to THAs by using multicast address. After receiving multicast packets, THAs will tunnel the multicast packets to MH's current FAs. FAs will complete multicast packets delivery to MHs by using link-level multicasting.

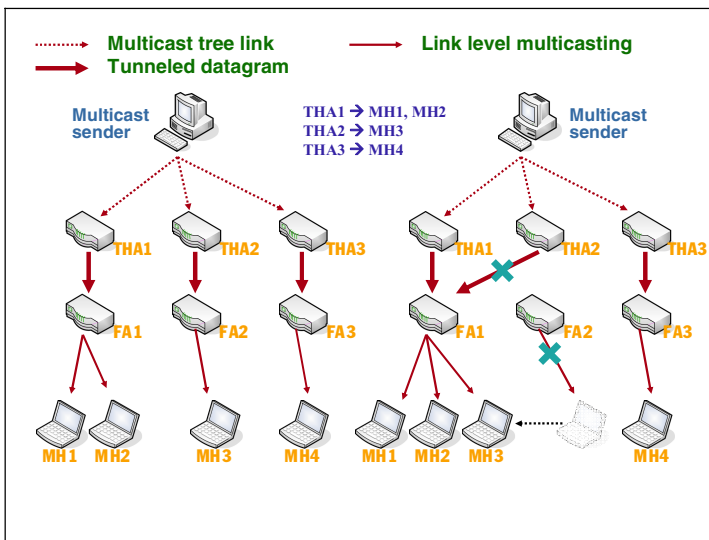


Fig. 2. HH-MIP/ME Data delivery

To avoid the duplication of multicast packets on the foreign network in the event that the THA has multiple MHs present there, just one copy of multicast datagram is sent to the foreign network and link-level multicasting is used by the FA to complete the delivery.

To solve the tunnel convergence problem, the FA will select one of the THAs as the DMSP, for a given multicast group. THAs that are not the DMSP for a given multicast group can suppress delivery down the tunnel using negative caching, as described in PIM [13]. DMSP handover must be performed in case the MH that owns current active DMSP moves from current network to another foreign network. For DMSP selection, we use the THA that has been in the THA list for the longest time.

In THA handover scenario, MH will have to rejoin multicast group (if new FA has not joined the multicast group yet) by sending IGMP [14]-[15] join message to reconstruct multicast tree. In case current network (new FA) is served by DMSP, THA will suppress the multicast delivery of serving DMSP by sending negative caching. After completing the multicast tree, multicast sender will send multicast datagram directly to THA. Multicast tree in old THA will be deleted if no other MHs required. In case that the MH's old THA is the DMSP for a group at the (previous) foreign network, a DMSP handoff is required to select new DMSP and to forward datagram to the remaining multicast group members (if any) at the (previous) foreign network. Until the DMSP handoff is completed, multicast delivery for group members at the foreign network will be disrupted. Fig. 3 illustrates the join message and data delivery during THA handover.

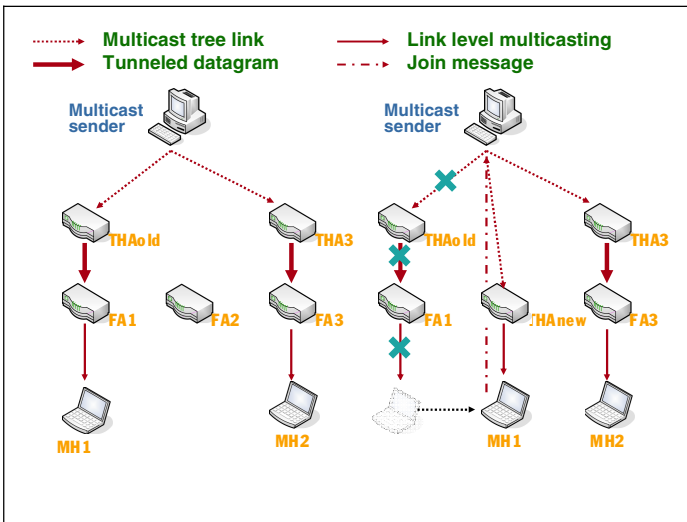


Fig. 3. Join message and data delivery during THA handover

3.2 Protocol Data Structure

In order to support HH-MIP/ME, data structures included in HH-MIP protocol must also be supported. These data structures include: (1) each HA must maintain an away

list. Away list is used to keep track of which of its own MHs are away and their current active THA, (2) each FA maintains a visitor list. Visitor list is used to keep track of which mobile hosts are currently at its LAN and their current active THAs, and (3) each THA must maintain Temporary Child List (TCL) to keep track of temporary MHs that THA has responsible, from where these mobile hosts come from and where these mobile hosts are. In HH-MIP, THA can be an FA or HA.

The HH-MIP/ME protocol also requires group membership information for the away and visiting MHs. Each THA Group Information keeps track of three things for each multicast group that it knows about: a list of away MHs that are members of the group, a list of the FAs at which the away group members reside, and a list of the FAs for which the THA has DMSP responsibilities. Similarly, each FA keeps track of three things on a per group basis: a list of visiting mobile hosts that are members of the multicast group, a list of the THAs to which these visiting group members belong, and a list of THAs that are currently serving as DMSPs for this group.

4 Performance Evaluation

4.1 Simulation Environment

The network topology in our simulation is 8 x 8 mesh network. Each node in the mesh represents an FA. The locations of the HA and multicast sender are randomly selected from the mesh. Initial locations for the MHs are also randomly selected from the mesh. In order to model the mobility of the MHs, time is slotted and the parameter called Movement Probability (*MoveProb*) [16] is used in the simulation. *MoveProb* represents the probability that an MH leaves its current network in the next slot time. Thus, we could model high mobility of MHs by assigning a large value of *MoveProb*. When an MH decides to leave the current network in the next slot time, its next foreign network is randomly selected from the neighboring networks. For simplicity of our simulation, there is only one multicast group in which only one multicast source is assumed. The number of MHs in multicast group varies from 10 to 50. We also simulate the protocols performance in different mobility pattern. Total run time in the simulation for each approach is 500 slot times.

4.2 Performance Criteria

In the performance evaluation, we compare our approach with MoM (bi-directional tunneling enhancement using DMSP) and remote subscription (RS). Both protocols have their own advantage and disadvantage. MoM is based on MIP which multicast packets are received by HA on behalf of MH. This approach handles source mobility as well as recipient mobility and in fact hides host mobility from all other members of the group. The disadvantages of this approach are the routing path for multicast delivery can be far from optimal and scalability problem. With remote subscription, the MH has to re-subscribe multicast group when it moves to other domain network. The main advantages of remote subscription are it is a simple protocol and it has the

optimal path for multicast packets delivery. The drawbacks for remote subscription are it introduces large signaling overhead and large packet loss as MH moves to different domain network.

Some criteria are used to compare the performance of our approach with other approaches:

1. **Average of the summation of end-to-end path length in a group.** In average of the summation of end-to-end path length in a group (in hop counts), we will measure the average number of hop counts the multicast packets travel from multicast source to each MH's current position. End-to-end path length is used to show the routing efficiency of the approaches. The longer the distance the packets travel from sender to destination means the larger the delay between sender and receiver. Approach with large end-to-end delay is not suitable for real time interactive applications.
2. **Tree maintenance overhead.** In tree maintenance overhead (in average number of control packets), we will measure the average number of join and leave messages have been sent during the simulation period. For HH-MIP/ME, *join* message is sent when MH arrives in new foreign network (FA has not joined multicast group membership yet) or when MH triggers the THA handover. *Leave* message is sent when MH leaves previous network and no other MHs use the multicast tree. Comparison will be made between HH-MIP/ME and remote subscription.
3. **Average number of DMSP handoff.** In average number of DMSP handoff (in number of DMSP handoff), we will measure the average number of DMSP handoff per MH handoff during the simulation period. Increase in DMSP handoff will introduce packet loss because packet loss will occur before DMSP handoff is completed. Comparison will be made between HH-MIP/ME and MoM.
4. **Average DMSP handoff latency.** In average DMSP handoff latency (in hop counts), we will measure the average number of hop counts the DMSP update message travels from foreign network to new selected DMSP. Longer path will induce larger packet loss caused by longer DMSP handoff time. Comparison will be made between HH-MIP/ME and MoM.

4.3 Simulation Results

The first simulation result is to evaluate the routing efficiency of different approaches. In average end-to-end path length, we compare the end-to-end routing path of multicast packets between each protocol. Fig. 4 shows the end-to-end path length of different protocols at different group member size. Remote subscription has the best performance compare to the other protocols because each multicast delivery is sent directly to its current foreign network. The HH-MIP/ME has a better performance than MoM because multicast packets are sent to the THA which resides near mobile host current position. As for MoM, it has the worst performance because of the triangular routing problem.

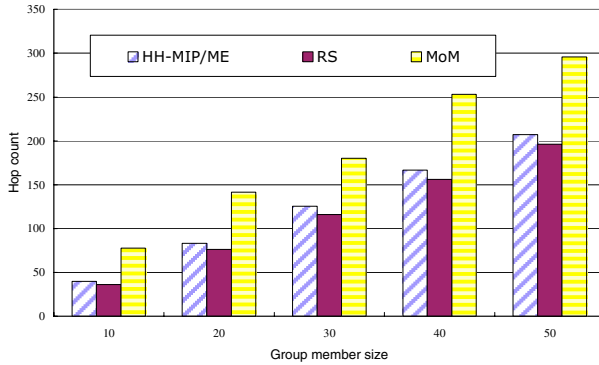


Fig. 4. Summation of end-to-end path length in a group

Fig. 5 compares the tree maintenance overhead between HH-MIP/ME and Remote Subscription. The overhead of concern is join and leave messages have been sent during multicast tree reconstruction. Remote Subscription introduces larger overhead because MH needs to send join message each time it moves to different network and sends leave message to quit from the tree. Obviously, the tree maintenance cost will increase when the mobility is getting higher. For the HH-MIP/ME, it reduces the overhead by reducing unnecessary tree reconstruction. The HH-MIP/ME will need to reconstruct multicast tree in case of THA handover. The HH-MIP/ME also performs well in case of high mobility.

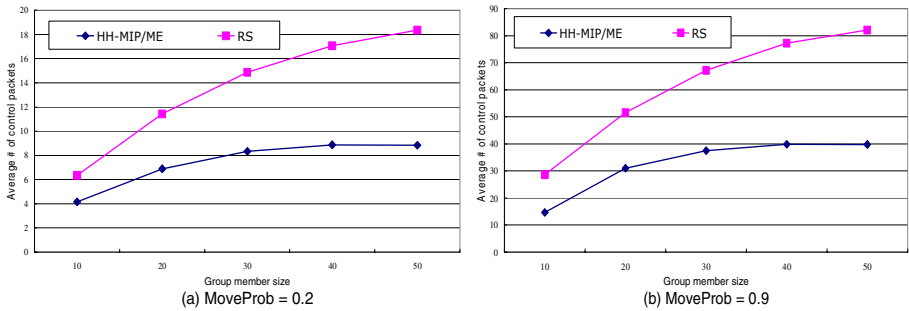


Fig. 5. Tree maintenance overhead at different MoveProb

Fig. 6 shows the average number of DMSP handoff during the total simulation period in HH-MIP/ME and MoM. In high mobility, the DMSP will handoff more frequently since MHs' handoff take place easily. MoM has fewer DMSP handover because HA that acts as DMSP is static. The DMSP will handoff only if the DMSP owner leaves its current network. The HH-MIP/ME has larger number of DMSP

handoff because THA handover has the chance to initiate the DMSP handoff. Number of DMSP handoff in both protocols will increase in case of high mobility.

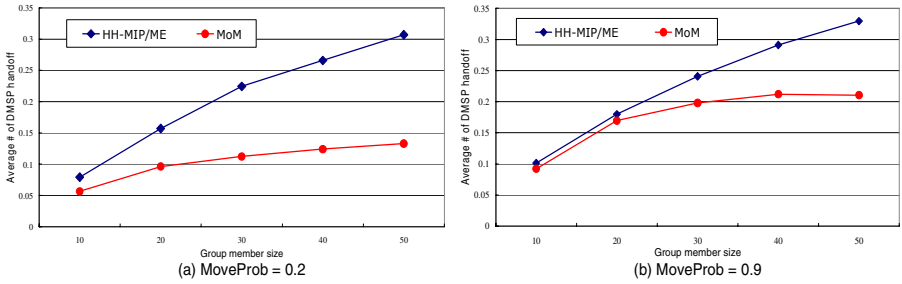


Fig. 6. Number of DMSP handoff at different MoveProb

When we compare Fig. 6 (a) with (b), we find out a very interesting phenomenon that the value of average number of DMSP handoff in Fig. 6 (b) is higher than value in Fig. 6 (a). As we normalize the average number of DMSP handoff with number of MH handoff, the value must be the same at both figures. In Fig. 7, we run simulations to obtain total number of DMSP handoff in different mobility pattern with group size = 10 for both protocols. In both simulations we find out that the value in y axis (total number of DMSP handoff) does not increase linearly in case of different mobility pattern. We assume that the phenomenon is caused by the complex mechanism in the DMSP selection.

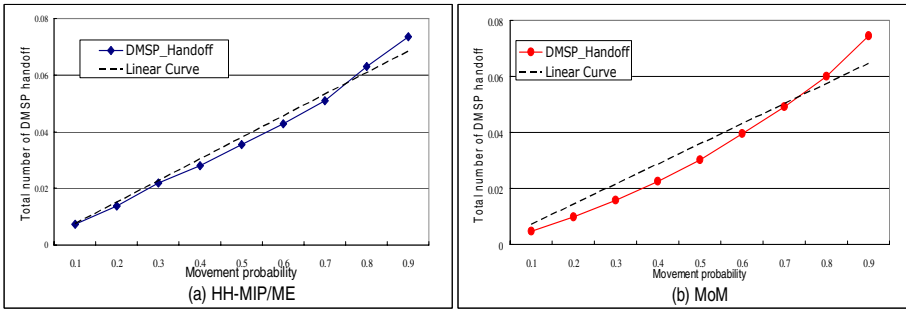


Fig. 7. HH-MIP/ME and MoM total number of DMSP Handoff

Fig. 8 shows the average DMSP handoff latency (in hop counts). The MoM has larger DMSP Handoff Latency because length of the path needs to update the new selected DMSP (HA) is longer in the MoM than HH-MIP/ME. The HH-MIP/ME has moderate DMSP Handoff Latency because MH's THA is resided near the MH current position.

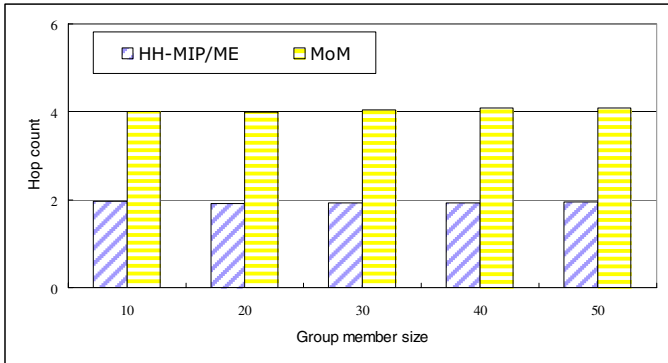


Fig. 8. DMSM handoff latency

5 Conclusion

The HH-MIP/ME as multicast extension of HH-MIP is presented in the paper. The HH-MIP/ME inherits the advantages of HH-MIP because it is built on the top of HH-MIP. The HH-MIP/ME uses its THA on behalf of MH to join the multicast group. Multicast packets are sent by multicast sender to MH's THA and the THA will tunnel to MH current position (FA). To avoid data duplication and tunnel convergence problem, the HH-MIP/ME uses DMSM concept. The simulation results also show that the HH-MIP/ME has better performance than existing protocols like the MoM and Remote Subscription.

Acknowledgments. This work was supported in part by the National Science Council, Taiwan, R.O.C., under grant NSC95-2219-E-260-004.

References

1. Akyildiz, I.F., Xie, J., Mohanty, S.: A Survey of Mobility Management in Next-Generation All-IP-based Wireless Networks. *IEEE Wireless Communications*, 16–28 (2004)
2. Perkins, C.E.: IP Mobility Support for IPv4. RFC 3344 (2002)
3. Johnson, D., Perkins, C.E., Arkko, J.: Mobility support in IPv6. RFC 3775 (2004)
4. Hwang, Y.-H., Chen, J.-Y., Yang, C.-C., Chen, W.-S.: A comparison between SIP and network layer mobility management protocols in wireless IP networks. In: *Proceedings of Fifth IEE International Conference on 3G Mobile Communication Technologies*, pp. 317–321 (2004)
5. Campbell, A.T., Gomez, J., Kim, S., Turányi, Z.R., Valkó, A.G., Wan, C.Y.: Internet micromobility. *Journal of High Speed Networks* 11(3-4), 177–198 (2002)
6. Perkins, C.E., Johnson, D.B.: Route Optimization in Mobile IP. draft-ietf-mobileipoptim-11.txt (2001)
7. Dell'Abate, M., De Marco, M., Trecordi, V.: Performance evaluation of Mobile IP protocols in a wireless environment. In: *Proceedings of 1998 IEEE International Conference on Communications*, pp. 1810–1816 (1998)

8. Yu, L.-S., Yang, C.-C.: An Enhancement of Mobile IP by Home Agent Handover. In: Proceedings of IEEE 62nd Semiannual Vehicular Technology Conference (2005)
9. Chikarmane, V., et al.: Multicast support for mobile hosts using mobile IP: Design issues and proposed architecture. *Mobile Networks and Applications* 3(3), 365–379 (1998)
10. Harrison, T., et al.: Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts. *ACM MOBICOM 97*, 151–160 (1997)
11. Ye, M.-H., et al.: The Implementation of Multicast in Mobile IP. In: Proceedings of WCNC 2003, pp. 1796–1800 (2003)
12. Lin, C.-R.: Mobile Multicast Support in IP Networks. In: *IEEE Global Telecommunication Conference*, vol. 2, pp. 1935–1939 (2002)
13. Deering, S., et al.: An Architecture for Wide-Area Multicast Routing. In: Proceedings of ACM SIGCOMM Conference, pp. 126–135 (1994)
14. Fenner, W.: Internet Group Management Protocol Version 2. RFC 2236 (1997)
15. Deering, S.: Host Extensions for IP Multicasting. RFC 1112 (1989)
16. Yang, C.-C., Lin, K.-Y.: Distributed Mobile Tracking: A Novel Location Management Scheme for Routing Improvement in Cellular IP Networks. *Journal of Computer Networks* 43(2), 141–167 (2003)

Autonomic Multi-server Distribution in Flash Crowds Alleviation Network

Merdan Atajanov¹, Toshihiko Shimokawa², and Norihiko Yoshida¹

¹ Graduate School of Science and Engineering
Saitama University

Saitama 338-8570, Japan

² Faculty of Information Science

Kyushu Sangyo University

Fukuoka 813-8503, Japan

Abstract. The Flash crowds are rapid increase in access to contents of web sites, which makes the web sites inaccessible, leaving the clients with unsatisfied requests. The major shortcoming of flash crowds researches is that they do not assist vital resizing feature of a cloud of the surrogates; the surrogates involved in the alleviation process do not change from the start to the end of flash crowds. Our system, FCAN (Flash Crowds Alleviation Network) is a system to provide resources to web sites to overcome flash crowds. A main feature of FCAN is its dynamically resizing feature, which can adapt to request load of flash crowds by enlarging or shrinking a cloud of surrogate servers used by the web sites. In this paper, we present a new feature of FCAN to support multiple servers which experience different flash crowds simultaneously, and show experiment results with real web log data provided by Live Eclipse 2006.

Keywords: Internet Load Distribution, Content Distribution Networks, Flash Crowds.

1 Introduction

Even though the Internet capacity and network bandwidth emerged very rapidly these days, in some cases clients still experience problems while accessing the web sites. These problems are slightly different from the problems that were in the early days of the Internet. These new problems involve network congestion, traffic bottleneck on the server side, which maybe caused by the overwhelming number of users simultaneously accessing web contents. This is called “flash crowds” phenomenon [1]. The best way to provide decent replies to the clients is to disseminate the requested contents as near as possible to the clients. Most of the corporations disseminate their web contents by implementing geographically distributed network of surrogate servers or by using services of the companies such as Akamai [2]. These companies distribute the load of highly hit web sites

across a geographically dispersed network in advance. Their solution mainly focuses on using proprietary networks and caching centers to intercept and serve clients requests before the flash crowds occur.

As a new solution, we already introduced a system called FCAN (Flash Crowds Alleviation Network) [3, 4]. It utilizes cache proxies in the Internet as surrogates to form an anti-flash crowds system. Its advantageous feature over other anti-flash crowds systems is that FCAN has a dynamic nature: with its help, a cloud of surrogates can grow or shrink adapting to the changes in traffic coming to the surrogates. Some small subset of cache proxies is involved at the beginning, and the subset can grow or shrink adapting to the load changes.

Our previous works were done considering just single server situation, where only one server can benefit from FCAN system. We extend our FCAN so that it can handle several member servers experiencing flash crowds. We focus our attention on addressing multi server situation, when several servers experience flash crowds simultaneously. Our system handles several flash crowds simultaneously by splitting a network of cache proxies to the servers that experience the flash crowds. The cache proxy can be involved in several flash crowds events, however the system tries to keep cache proxies involvement only in one flash crowds' event. In this paper, we use real flash crowds' data to investigate how FCAN behaves more realistically than in [4]. First we provide simulation results with artificial data and then show results with real flash crowds' data.

The rest of the paper is organized as follows: Section 2 is Related Work section; in Section 3, we describe FCAN design. The simulation data and results are in Section 4. Section 5 is the conclusion, including some considerations and future work.

2 Related Work

The flash crowds event is a very recent phenomenon in the Internet. Mostly flash crowds are infrequent and unpredictable events: you can predict that flash crowds could happen, but it is almost impossible to predict their magnitude and duration. Related researches against flash crowds can be divided into three categories: server-based solutions, client-based solutions, and intermediate solutions.

The CDN (Content Distribution Networks) is one approach in server-layer solutions. The main idea is to distribute load expected for one server to several surrogate servers. The server-layer solution's biggest disadvantage is over-estimation of resources; these resources are only used in the flash crowds' event. In most cases, a flash crowds event is unexpected or unpredictable, it takes short time; therefore providing extra resources is not a good solution to anticipate flash crowds. In the client-side solutions client transparency is gone which in most cases requires client cooperation. Moreover the client-side solutions are very difficult to manage. Related work against the flash crowds includes Coral-CDN [5] and P2P-based systems such as Backslash [6] and PROOFS [7]. Main characteristics of flash crowds are extensively studied in [3], these characteristics were used as the basis for designing FCAN system.

3 FCAN Design

3.1 Overview

FCAN is an intermediate layer solution, focusing on a CDN-like cloud of cache proxies where popular objects are cached in, and delivered to end users. Our proposal is to construct the CDN-like cloud of proxies where all proxies are static members. This cloud of CPs (cache proxies) is widely spread with lots of participants. When flash crowds occur, the member server chooses a subset of proxies to form its small cloud, which will be responsible for the popular objects. If the subset of CPs cannot handle the client requests, new proxies are invited and the cloud grows. When the flash crowds decrease, cloud of CPs shrinks.

The popular objects are stored in some kind of CDN-like cloud of reverse proxies. In these proxies, contents are stored for the duration that flash crowds last, and client requests that are supposed to go to the server, are delivered to these proxies serving as surrogates. In this way, the load on the main server is reduced, and more clients get satisfied replies. In the peaceful time, there is no need for the FCAN system to be active; it is only activated when flash crowds occur, and it helps servers until the flash crowds are over. DNS redirection is used to redirect client requests to the cache proxies.

FCAN consists of the below:

- A member server: is a server that suffers from the FC (flash crowds) event and wants to use system to overcome it.
- A FC object: is a main content that is requested in flash crowds' event.
- A Permanent proxy member: is a main proxy in the CDN-like cloud. It is divided into two subgroups:
 - A Core proxy member: is a proxy that is always responsible for a FC object, when the member server is in FC state.
 - A Free proxy member: is a proxy that dynamically joins and leaves the core part, and helps the core proxies when they are overloaded.

Every proxy can be a core or a free proxy, it can even be a core proxy for one member server and a free for another member server. The free proxies stay alert in case any of member servers begin to experience flash crowds. In that case some of the CPs switch to the core proxy state and help the member server.

3.2 Key Features of FCAN

The proxies generate and monitor such statistical information as request rates and loads for the FC objects. These statistics are passed to and processed by the member servers to monitor the overall state in alleviation procedure so that the member servers decide when to enlarge or shrink the cloud, and find out when the flash crowds are over.

All permanent proxies are defined beforehand and configured by the administrator of the system. These proxies form main CDN-like cloud of CPs, which is used by the member servers that suffer from flash crowds. Every permanent proxy should provide the following functions:

Table 1. Priority Table for the member servers

| | SVR01 | SVR02 |
|-----|-------|-------|
| CP0 | 70 | 90 |
| CP1 | 20 | 50 |
| CP2 | 10 | 100 |
| CP3 | 30 | 30 |
| CP4 | 90 | 20 |
| CP5 | 60 | 40 |
| CP6 | 100 | 10 |
| CP7 | 50 | 80 |
| CP8 | 40 | 70 |
| CP9 | 80 | 60 |

- Change its state from a free proxy member to a core proxy member and vice versa
- Distribute permanent proxy database list
- Provide ability to store FC objects permanently
- Generate and monitor statistics of request rate and load
- Maintain cloud membership operations

The proxy has an ability to store FC objects permanently; these objects do not expire until FC event is over. The member server has the following functions:

- Disseminate FC object to the core proxies
- Manage own core set of proxies involved
- Trigger an update of DNS zone file
- Collect and process statistics generated by the core proxies

FCAN system uses a priority table in the selection mechanism of proxies. As it can be seen in the Table 1, the cache proxies are assigned different priorities for different member servers, where the least number has the highest priority. FCAN system assigns proxies to member servers according to these priorities.

The priorities are not sequential, but sparse. A new additional proxy can be easily inserted in between, or be removed from the table without a need to update priorities.

The core proxies' IP addresses are added to the DNS record of the member server, so that requests are redirected to the core proxies. While DNS update propagates, all the requests are still going to the member server. The member server can act beforehand, by triggering DNS update before state change of the FCAN system. This way DNS propagation will catch up sooner. Load distribution is done by round-robin DNS, or it may be done by some other advanced selection mechanism [8].

3.3 Overall View

At first, the system is in a peaceful state in which there are no flash crowds as it is shown in the left of Figure 1, and FCAN is in an inactive mode. When

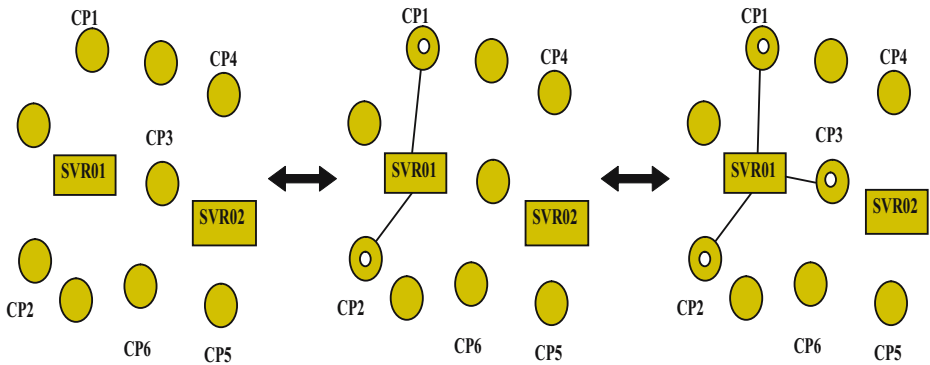


Fig. 1. FCAN Outline

flash crowds come, a system forms a CDN-like cloud of core proxies, which act as surrogates for the member server as shown in the middle of Figure 1. If the cloud of surrogates cannot handle increasing amount of requests for the FC object, the member server invites more free proxies to participate in the cloud as shown in the right of Figure 1.

The member server selects potential core proxies among the proxies by sending check requests to these proxies. First, it probes a proxy which has the highest priority for the member server, and then a proxy with the second highest priority, and so on. Eliminating proxies which are already used in other servers' flash crowds alleviation procedure. This way it will find the most appropriate proxies that can participate in the alleviation procedure. When potential candidates are selected, the member server triggers DNS update to include IP addresses of newly added proxies, and disseminates FC object(s) to the selected proxies. In Figure 1, the initial core cloud consists of two proxies, CP1 and CP2.

3.4 The Cloud Growth and Shrinkage

There are two thresholds used in the FCAN system: T_{high} and T_{low} .

- T_{high} : the request rate is close to critical or soon will be above the acceptable rate, so that the system switches its state to the CDN-like cloud of the cache proxies.
- T_{low} : request rate is low, so that the system switches its state back to the peaceful client/server state.

When a member server detects that the load exceeds T_{high} , the system becomes active. When the initial core cloud is not enough, a new proxy (CP3 in Figure 1) is added to already involved member proxies (CP1 and CP2), and CP3 becomes core proxy for SVR01. When the average load on the core proxies is below T_{low} for predefined duration, the member server concludes that FC event is over. So, at first, it dismisses only some of the core proxies, and updates DNS.

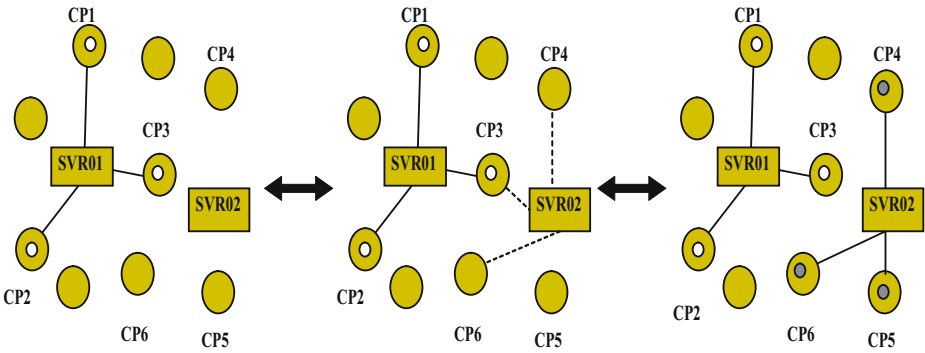


Fig. 2. Multiple Member Servers in FCAN

The proxies with the lowest priority are dismissed first. Then, if the request rate at proxies is still under T_{low} , the member server dismisses some other core proxies. This process continues until all core proxies are dismissed. Firstly, the DNS records are updated, and the proxies wait for certain period until DNS propagation is supposedly finished. Then they change their state from core to free. The DNS redirection is done before dismiss, so as to prevent client requests being redirected to the proxy which does not have the flash crowds content, or which already changes its state to a normal forward proxy.

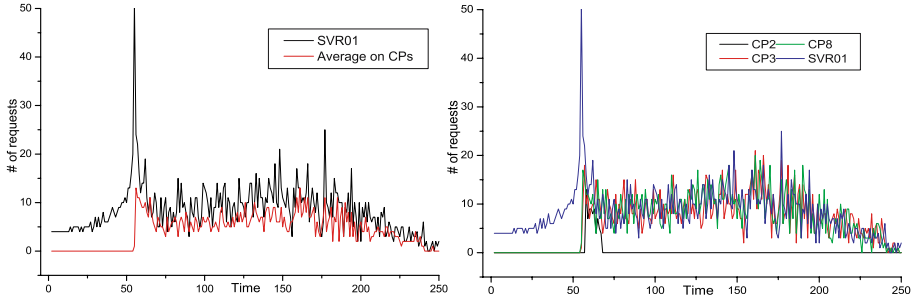
3.5 Multi-server Scenario

Cache proxies and member servers are independent from each other. FCAN is not designed for some specific member servers; it is designed to be used by several member servers in need at the same time. A member server can use a subset of proxies depending on the magnitude of flash crowds, and another member server can use another subset of the proxies. A proxy in the system can be a core proxy for one member server and a free proxy for another server. It is preferable that these subsets of the proxies used in different flash crowds do not overlap. To avoid overlapping, the system uses the priority table with predefined priorities for the member servers. When flash crowds comes, proxies are assigned to member servers according the priorities. If the proxy is already used in another flash crowds alleviation process, FCAN skips it and moves to a next proxy in the priority table.

In Figure 2, suppose that SVR02 also starts to experience the flash crowds event. It needs to construct its own cloud. Let assume that flash crowds magnitude of SVR02 is higher than SVR01, therefore the system invites three proxies at the beginning. From the table 1, we see that initially CP3 is overlapping between SVR01’s core proxies cloud and SVR02’s. However CP3 is already used in alleviation process for SVR01’s flash crowds. So, when SVR02 probes CP3, it finds out that CP3 is busy, so it leaves CP3 and invites a next proxy from

Table 2. Simulation with Artificial Input

| Servers | Start (sec) | End (sec) | CPs used | Initial Set | T_{high} (req/sec) | T_{low} (req/sec) |
|---------|-------------|-----------|----------|-------------|----------------------|---------------------|
| SVR01 | 55 | 250 | 8,3,2 | 8,3 | 40 | 5 |
| SVR02 | 45 | 175 | 0,6,4 | 0 | 30 | 5 |

**Fig. 3.** SVR01 with artificial input

the priority table, which is CP5. After the initial core cloud is defined, SVR02 disseminates contents to its core members. These measures are done to avoid overlapping of the core proxy clouds.

In case where all proxies are used up in the alleviation procedure, some member server should share some of the proxies among each other. The proxies that are shared among member servers will divide local capacity per server to be able to handle the requests for several flash crowds' objects.

4 Simulation and Results

Our simulation has three roles: member servers, member proxies, and clients; each of them runs as independent thread. It is based on previous simulation of FCAN project. The network is built on an application layer with servers and proxies running continuously and concurrently. Clients' threads are created to send the requests, and then destroyed after getting the replies. Either a server or a proxy rejects the incoming requests if the average load exceeds its capacity. When the traffic is increasing, a member server switches the system to CDN-like cloud of proxies. If the initial core proxies are not enough in the alleviation procedure, the member server invites new proxies, until the load is stabilized. When the load is decreasing, the proxies begin to leave the cloud and a member server is switched back to the normal state.

Table 2 summarizes the configuration for the simulation of servers SVR01 and SVR02 with artificial input. Figures 3 and 4 present the results of this simulation. The left graphs in Figures 3 and 4 show average load, while the right graphs show individual loads on the proxies and member servers. The flash crowds for SVR01

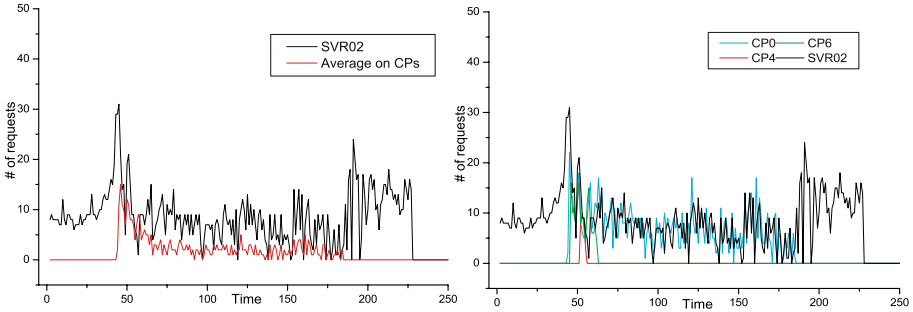


Fig. 4. SVR02 with artificial input

Table 3. Simulation Configuration

| | |
|--|---------------------|
| Servers involved | 2 |
| The number of proxies | 10 |
| Proxy's priority order for SVR01 | 8,3,2,5,7,1,9,4,6,0 |
| Initial set for SVR01 | 8,3 |
| Proxy's priority order for SVR02 | 0,6,4,9,1,7,5,2,3,8 |
| Initial set for SVR02 | 0 |
| Threshold T_{high} (req/sec) for SVR01 | 30 |
| Threshold T_{low} (req/sec) for SVR01 | 5 |
| Threshold T_{high} (req/sec) for SVR02 | 20 |
| Threshold T_{low} (req/sec) for SVR02 | 5 |
| Server Capacity (req/sec) SVR01 | 40 |
| Server Capacity (req/sec) SVR02 | 30 |

start at 55th second and continue until the end of simulation. The flash crowds for SVR02 start at 45th second and end at 175th second. The magnitudes of two flash crowds are different; the magnitude of SVR01's flash crowds is bigger than the SVR02's. Three additional proxies CP8, CP3, CP2 are used till the end of the SVR01's flash crowds. On the other hand only CP0 is used till the end of the SVR02's flash crowds and CP6, CP4 is used just for 10 seconds at the beginning of the flash crowds.

Next, we investigate simulation results with real access logs, kindly provided by "Live Eclipse" web site [9]. These live web logs are used as the input data for simulation with multi-server scenario. In March 2006, Live Eclipse delivered web streaming for the Eclipse that took place in Turkey, Libya and Egypt. Live Universe provided two different streaming sites:

- <http://www.live-eclipse.org>
- <http://www.nishoku.jp>

The first one was used by all the clients in the world, while the second one was just by Japanese clients. Therefore, there is a difference in access graphs for

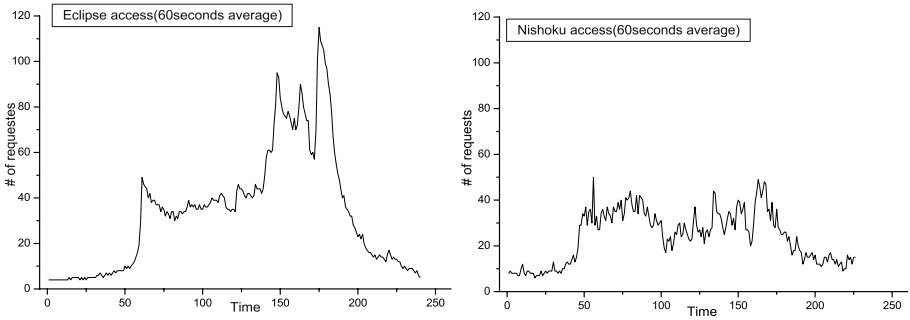


Fig. 5. Access Pattern for “Live-Eclipse” and “Nishoku” Sites

these two sites, as expected access rates for the live-eclipse is much higher than for the nishoku site. Figure 5 shows access rate patterns for these two sites at the time eclipse took place.

The logs for these two servers are scaled down so we can feed them into the simulation. The log of Live-Eclipse site is scaled down by 30, and log for Nishoku site by 10. Every simulation second corresponds to one minute of real time.

In this experiment, two different member are used servers one for live-eclipse, another for nishoku and also ten permanent proxies are used for alleviation procedure. Table 3 summarizes the configuration of ten proxies and two independent member servers. The SVR01 and SVR02 experience flash crowds at the same time: SVR01 is fed the live-eclipse log, and SVR02 is fed the nishoku log. The priorities for these member servers are different, and initial core sets of proxies are different between the member servers according to their priority settings for the proxies and magnitudes of flash crowds. Before inviting free proxy to join the core cloud, a member server checks if free proxy is available, not used in other member server’s flash crowds event. If it is already used by another member server, then a next free proxy in the priority table is probed for availability.

Figure 6 and 7 shows the results of the simulation with real data, where Figure 6 shows SVR01 “Live Eclipse” server’s cloud and Figure 7 shows SVR02 “Nishoku” server’s cloud. The left graphs in Figures 6 and 7 show average load, while the right graphs show individual loads.

For SVR01, seven proxies are used: two core proxies and five additional proxies. Initial set of the core proxies consists of two proxies CP8 and CP3. For the first 60 seconds the member server can handle the client requests itself. The SVR01’s flash crowds start around 60th second. The member server invites initial core set of proxies to join in the alleviation process. At the beginning the requests grow so rapidly that initially assigned two proxies are not enough. Therefore third proxy CP2 is added to the system immediately. In this situation where three proxies and member server are involved, the system handles the load until the next rapid increase of flash crowds starting around 150th second. Four more proxies are added to the system in the following order: CP5, CP7, CP1, and CP9. With the help of these new additional proxies to the core part, the average

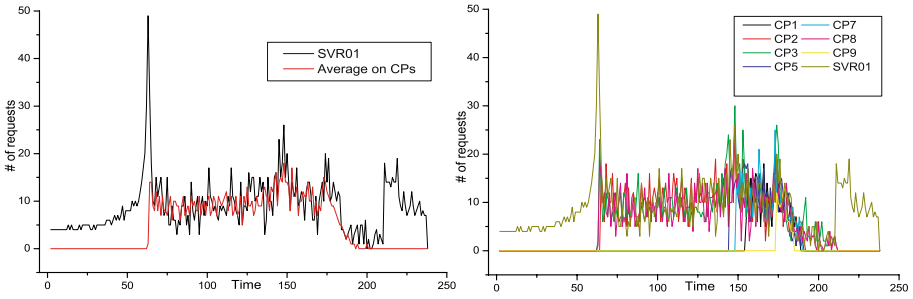


Fig. 6. Access Log of “Live Eclipse” Proxy Cloud

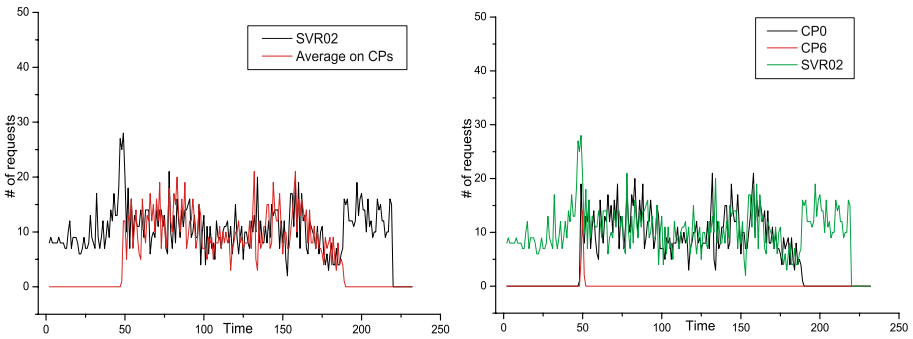


Fig. 7. Access Log of “Nishoku” Proxy Cloud

load on the system is kept under the threshold Table 3. After 180th second, the client requests start decreasing very rapidly. At this moment, the system waits short duration to check if it is temporary change in the client requests. Since requests are decreasing at the steady rate, the system dismisses the proxies one by one until the system is switched back to the client/server mode. The state change occurs around 200th second.

In Figure 7, SVR02 uses two proxies, one is core proxy and the other is additional free proxy. Initial set consists of just one core proxy CP0. The SVR02’s flash crowds start around 50th second, at this point, the highest peak of client requests is reached. Initially CP0 is added to the system, then immediately CP6 is invited for 3 seconds. The CP6 is dismissed since the load is not high and can be handled by one core proxy and member server. In this situation where just one core proxy and member server are involved, the system handles all client requests until the end of the flash crowds. The SVR02’s flash crowds ends around the 195th second. The member server dismisses core proxy CP0 and switches back to normal client/server mode.

5 Discussions

The flash crowds are very unpredictable events. Therefore it is very difficult to determine T_{low} and especially T_{high} thresholds. T_{low} should be as low as average load of the server in peaceful time. But the system will not switch itself to C/S mode, just by load dropping under T_{low} . The load should persist under T_{low} for predefined duration of time. T_{high} is defined as the rate that is reached in a short duration, and which cannot be handled by the member server itself. At the moment it is planned that CPs are volunteer proxy servers that are already functioning on the Internet. The priority assignment to individual CPs is done beforehand; priorities are in the way so that a proxy is not assigned high values for several member servers. This way we reduce overlapping of the proxies involved in the alleviation procedure. The selection of CPs for a member server depends on the priorities assigned to proxies for that member server. Before assigning the proxy as a core proxy, the member server probes the proxy for availability and checks if it is not used by any other member server. In case the proxy is involved in another alleviation procedure, the member server skips to the next proxy in the priority table.

6 Conclusions

The strong point of FCAN is its dynamically resizing feature for the cloud of surrogates. This cloud can grow or shrink according to the load of the system. In this paper, we present FCAN's support for multiple servers simultaneously experiencing independent flash crowds. We investigate efficiency of this feature using real data which were kindly provided by Live Eclipse project. The simulation results showed that FCAN system is capable of handling multiple flash crowds at the same time.

In the Internet, dynamically generated contents have become more and more popular. We are planning to concentrate our attention on dynamic contents in flash crowds. The dynamic contents can be divided into two categories:

- Dynamically generated objects (using a backend database and scripts)
- Frequently updated contents

It is important to reduce the number of messages and amount of data exchanged in the network to reduce network congestion. In the flash crowds event, the network already will be overwhelmed by flash crowds object.

Now we are applying some techniques originally developed for “distributed shared memory”, especially the “lazy release consistency” technique which was proved one of the most efficient [10].

Acknowledgments

This research was supported in part by MEXT in Japan under Grants-in-Aid for Scientific Research on Priority Area 18049009, and by JSPS in Japan under Grants-in-Aid for Scientific Research (B) 17300012.

References

- [1] Flash Crowd phenomenon, http://en.wikipedia.org/wiki/Flash_Crowd
- [2] Akamai, <http://www.akamai.com>
- [3] Pan, C., Atajanov, M., Hossain, M.B., Shimokawa, T., Yoshida, N.: FCAN: Flash Crowds Alleviation Network Using Adaptive P2P Overlay of Cache Proxies. *IE-ICE Trans. on Communications* E89-B(4), 1119–1126 (2006)
- [4] Atajanov, M., Pan, C., Shimokawa, T., Yoshida, N.: Scalable Cloud of Cache Proxies for Flash Crowds Alleviation Network. *Int'l Trans. on Communication and Signal Processing* 8(1), 59–70 (2006)
- [5] Freedman, M.J., Freudenthal, E., Mazieres, D.: Democratizing Content Publication with Coral. In: *Proc. 1st USENIX/ACM Symp. on Networked Systems Design and Implementation* (2004)
- [6] Standing, T., Maniatis, P., Baker, M.: Peer-to-Peer Caching Schemes to Address Flash Crowds. In: *Proc. 1st Int'l Workshop on Peer-to-Peer Systems*, pp. 203–213 (2002)
- [7] Starvrou, A., Rubenstein, D., Sahu, S.: A lightweight, robust P2P system to handle flash crowds. *IEEE Journal on Selected Areas in Communications* 22(1) (2004)
- [8] Shimokawa, T., Yoshida, N., Ushijima, K.: DNS-based Mechanism for Policy-added Server Selection. In: *SSGRR 2000. Int'l Conf. on Advances in Infrastructure for Electronic Business, Science, and Education on the Internet* (July 2000)
- [9] Live Eclipse (2006), http://www.live-eclipse.org/index_e.html
- [10] Keleher, P., Cox, A.L., Zwaenepoel, W.: Lazy Release Consistency for Software Distributed Shared Memory. In: *Proc. 19th Annual Int'l Symp. on Computer Architecture* (1992)

Generic Energy-Efficient Geographic Routing for Ad-Hoc Wireless Networks

Chao-Lieh Chen¹, Jeng-Wei Lee², Cheng-Zh Lin³, Yi-Tsung Chen²,
Jar-Shone Ker³, and Yau-Hwang Kuo²

¹ Department of Electronic Engineering
Kun-Shan University, Yung-Kang, Tainan County, Taiwan
frederic@ieee.org

² Department of Computer Science and Information Engineering
National Cheng Kung University, Tainan City, Taiwan
{lijw,nose,kuoyh}@cad.csie.ncku.edu.tw

³ Advance Multimedia Internet Technology (AMIT) Corp.
Tainan County, Taiwan
{tomm,james}@amt.com.tw

Abstract. The proposed energy-efficient geographical routing (EGR) mechanism is generally applicable to reduce energy consumption in wireless communication networks. No matter for table-driven or on-demand ad-hoc routing algorithms, EGR enhances them by constructing an initial routing path considering location information. Then, to further improve energy utilization it selects relay nodes of links on the initial path. The EGR finds an optimum relay node in a relay region between any two traffic nodes to conserve energy and balance traffic load. The relay region is derived from the radio propagation model constraining energy-saving when relaying transmissions between two nodes. Any node within this region is a relaying candidate to decrease total traffic energy consumption and to balance traffic load. According to the Energy-Proportional Principle (EPP), we also propose an energy-saving criterion. To balance traffic load, the EGR follows the EPP and in the relay region selects the relay node with the highest score corresponding to the criterion. Compared to the traditional routing methods, EGR effectively utilizes energy and prolongs network lifetime.

Keywords: Geographic Routing, Ad-hoc Wireless Networks, Energy Proportional Principle, Load Balance.

1 Introduction

The classification of ad-hoc routing algorithms includes on-demand and table-lookup driven classes. The most representative routing protocols of these two classes are the Ad hoc On-demand Distance Vector (AODV) routing [5] and Destination-Sequenced Distance Vector (DSDV) routing [11] respectively. In AODV, nodes use the maximum transmission range to communicate with each other, but nodes can

adaptively adjust their power level for conserving transmitting energy by the Transmit Power Control (TPC) [1]. Lower power level means reduced interference problems and increased energy utilization. Namely, an energy-efficient routing protocol should be able to control transmission power dynamically. For load sharing and energy-saving, two communication nodes should dynamically tune down transmitting power when there are suitable relay nodes for the communication. The same situation happens in table-lookup driven routing algorithms such as DSDV. The routing table construction should consider the load sharing and energy saving especially when the location information is available.

In this paper we propose the Energy-efficient Geographical Routing (EGR) algorithm which is generally applicable to reduce energy consumption in wireless communication networks. The proposed EGR improves energy efficiency and load balance for both classes of ad-hoc routing algorithms. While a traditional routing protocol finds the routes in the path, EGR uses location information for initial path construction and then finds more route nodes in the initial routing path to minimize the total energy consumption. Since many later algorithms are developed from the two classes of ad-hoc routing, the EGR is a generic energy-efficient mechanism that is applicable to wireless networks.

We illustrate the geographical routing as examples. To extend the lifetime of the ad-hoc wireless networks, many articles proposed geographic routing as LAR [6] and GEAR [8] use location information to find a better routing path for saving transmission energy. Further, using energy-aware routing protocols like GAF [4] and SPAN [7] can save more energy consumption. The main idea is that they choose a node in a region as a coordinator to forward data, and other nodes go to sleep. Among them, Geographical Adaptive Fidelity (GAF) is one of the most representative routing algorithms that effectively use geographic information for coordinator selections and sleep-time scheduling for energy conservation. GAF divides the communication area into geographic grids. Though the grids ensure that all the nodes in a grid square are able to connect other nodes in any adjacent grid square, energy constraint in radio propagation is not considered. Therefore, any communication between two grids could violate the constraint and degrade performance in energy conservation. As an application, the proposed EGR improves energy conservation in wireless ad-hoc networks by constraining relay nodes selection while at the same time balances traffic load by applying the energy-proportional principle (EPP) in the relaying. The EPP originates from the energy-proportional routing [2][3], which effectively balance intra- and inter-cluster energy utilization and thus extend lifetime of clustered sensor networks. The EPP considers the total energy-proportional balance among nodes, rather than either merely simple balance of energy consumption or communication distance. In this way, the EGR effectively utilizes energy, balances the load, and thus prolongs network lifetime.

The paper is organized as follows. In Section 2, we reduce the relay inequality to a circular relay region and analyze the optimum number of the relay node. Section 3 depicts the construction process of EGR algorithm. Section 4 shows the experimental results of energy utilization. Finally, we give conclusions in section 5.

2 Energy of Radio Model and Relay Constraint

2.1 Energy Consumption and Propagation Model

In this paper, we apply the first order radio model commonly used in low-energy radios. When two nodes are d meters apart and sender transmits k bits data to receiver, the energy consumption can be calculated as follows [10] :

$$\begin{aligned} E_{Tx}(k, d) &= E_{Tx,elec} \times k + E_{Tx,amp} \times k \\ E_{Rx}(k) &= E_{Rx,elec} \times k \end{aligned} \quad (1)$$

The radio dissipates $E_{Tx,elec}$ or $E_{Rx,elec}$ in transmitting or receiving one bit data. $E_{Tx,amp}$ is depleted in amplifier for transmitting data, and determined by crossover distance (d_0). At the crossover distance, the power for receiving predicted by the two-ray ground (TR) reflection model equals to that predicted by the free-space (FS) propagation model. If the transmitter is within the crossover range, using the FS model is appropriate. Otherwise, use the TR model. That is,

$$E_{Tx,amp}(d) = \begin{cases} \varepsilon_{FS} \times d^2, & \text{when } d \leq d_0 \\ \varepsilon_{TR} \times d^4, & \text{when } d > d_0 \end{cases} \quad (2)$$

where ε_{FS} and ε_{TR} are the respective amplifier parameters in FS and TR models. In our simulation, we set the communication energy parameters as: $E_{Tx,elec} = E_{Rx,elec} = 50$ nJ/bit, $\varepsilon_{FS} = 100$ pJ/bit/m², $\varepsilon_{TR} = 0.013$ pJ/bit/m⁴ and $d_0 = \sqrt{\varepsilon_{FS} / \varepsilon_{TR}}$. Moreover, we let $\alpha_t = E_{Tx,elec} = E_{Rx,elec}$ and $\alpha_{amp} = \varepsilon_{FS}$.

2.2 Relay Region

Considering a simple illustration shown in Fig. 1, suppose that there are three nodes A, B and C. Assume all nodes use the same circuitry for transmission and receiving. The source node A sends data to the destination node B. For simplification, node A is located at the origin and B with coordinate $(d, 0)$ is d meters apart from node A. The

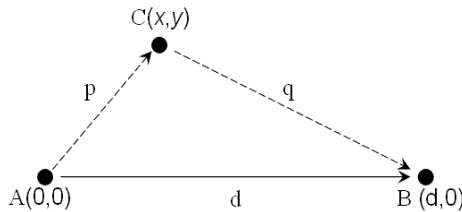


Fig. 1. Traffic from A to B

coordinate of relay node C is set to (x, y) . Assume C is p meters apart from A and q meters apart from B. For power saving, node C must be in a region to satisfy the following inequality (we call the region *relay region*):

$$(\alpha_t + \alpha_{amp}d^2) + \alpha_t > (\alpha_t + \alpha_{amp}p^2) + (\alpha_t + \alpha_t + \alpha_{amp}q^2) + \alpha_t$$

where the right hand side is the energy dissipation spent by the three nodes when using C for relay and the left hand side is the energy dissipation spent by the node A and node B when A send data directly to B. Substituting the coordinates into distances $d, p,$ and $q,$ we have

$$p^2 + q^2 < d^2 - \frac{2\alpha_t}{\alpha_{amp}}$$

$$\Rightarrow (x^2 + y^2) + [(d-x)^2 + y^2] < d^2 - \frac{2\alpha_t}{\alpha_{amp}}$$

Thus, we have the relay inequality (3) be reduced to a circular relay region.

$$x^2 - d \times x + y^2 + \frac{\alpha_t}{\alpha_{amp}} < 0 \tag{3}$$

Since the inequality is based on the FS model, the derived region is smaller than that derived from the TR model. Therefore, a relay node satisfies the inequality must also satisfy the one derived from the TR model. We focus on the smaller relay region through out this paper. Further, we study the relay region properties. The relay node in different location could result in different amount of *total saved energy* (E_s) which is defined as the energy saved by relaying and is obtained by subtracting the energy using relay from the energy consumption of direct transmission without relay. Therefore, we have

$$E_s = k \times \left\{ \left[(\alpha_t + \alpha_{amp}d^2) + \alpha_t \right] - \left[(\alpha_t + \alpha_{amp}p^2) + (\alpha_t + \alpha_t + \alpha_{amp}q^2) + \alpha_t \right] \right\}$$

In a general case, let A = (x_1, y_1) , B = (x_3, y_3) and C = (x_2, y_2) . We have

$$E_s = k \left[\alpha_{amp}(d^2 - p^2 - q^2) - 2\alpha_t \right]$$

$$= 2k \left[\alpha_{amp}((x_3 - x_2)(x_2 - x_1) + (y_3 - y_2)(y_2 - y_1)) - \alpha_t \right] \tag{4}$$

Fig. 2 shows the one-bit E_s of relaying when d is 250 meters and the relay node in the center of the source and the destination saves maximum E_s .

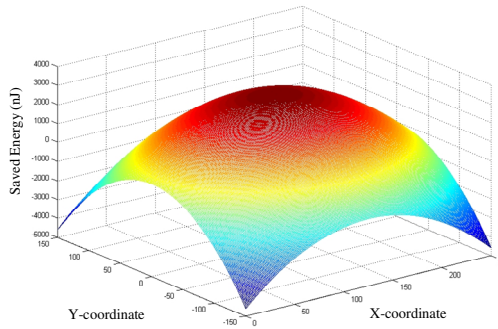


Fig. 2. Saved energy E_S on the geographical plane

2.3 Optimal Number of Relay Nodes

Though the more relay nodes satisfying the inequality the more power is saved, the more relay nodes in the traffic means the more delay time. So we need to find out the optimal number of relay node in trade-off between the two variables -- *total consumed energy* (E) and *delay time* (D). Let the optimal number of relay node is denoted as N_{opt} . Because E and D use different measurement units, we normalize two variables in advance and minimize the following weighted performance index to evaluate N_{opt} .

$$\beta E_{normalize} + (1 - \beta) D_{normalize} \tag{5}$$

In (5), β is the weight representing importance of *total consumed energy* and $E_{normalize}$ and $D_{normalize}$ are defined as following equations:

$$E_{normalize} = \frac{E|_{N=N_{opt}}}{E_{direct}} = \frac{(2N_{opt} + 1)\alpha_t + (d_{max}^2 / (N_{opt} + 1))\alpha_{amp}}{\alpha_t + \alpha_{amp} d_{max}^2} \tag{6}$$

$$D_{normalize} = \frac{N_{opt} + 1}{N_{MIN(E)} + 1} \tag{7}$$

We use an example to explain (6) and (7). Suppose that a node’s maximum communication range is d_{max} . For finding the upper bound of N_{opt} , the source is d_{max} meters apart from destination. There are N relay nodes in the routing path and the distance of every one-hop link is the same as $d_{max}/(N+1)$. E of N follows (1) and estimates total energy consumption. Moreover, since adding relay nodes reduces energy consumption E , the maximum value of E is E_{direct} when the source directly sends data to the destination. The delay D is proportional to the number of the hops. Because it’s impossible to add infinite relay nodes in the routing path, we calculate E of N as shown in Fig. 3 to find $N_{MIN(E)}$. When the number of relaying hops N is large than $N_{MIN(E)}$, both E and D increase. In this case $N_{MIN(E)}$ is 7 with $d_{max} = 250$.

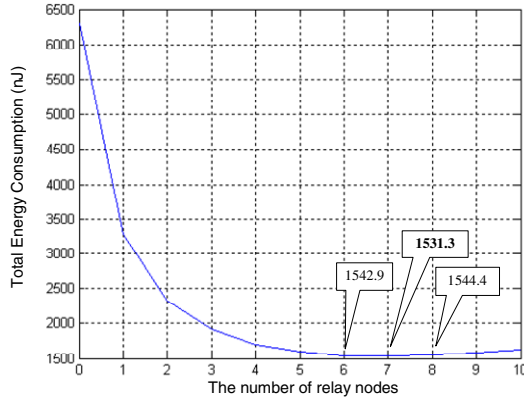


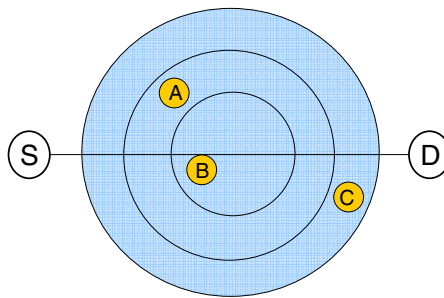
Fig. 3. When d_{max} is 250 metres, the number of relay nodes causes different total energy consumption

Therefore, we find $N_{opt} = 1.65$ when we minimize (5) subject to $\beta = 0.5$ and the above conditions. Consequently, we pick only one relay node in the relay region.

3 Construction of EGR

3.1 Selection of Relay Nodes

In Section 2, we know there is one relay node at most in a relay region. EGR picks the most proper node to relay data. The location of nodes affects the probability of being chosen by EGR. We substitute the location coordinates of nodes to (4) and choose the relay node having maximum E_S . However, a node having high E_S is expected to be



| | E_S (nJ) | SE -Ratio | E_R (J) | RE -Ratio | Relay-Score |
|---|------------|-------------|-----------|-------------|-------------|
| A | 1500 | 0.33 | 50 | 0.2 | 0.066 |
| B | 2300 | 0.51 | 100 | 0.4 | 0.164 |
| C | 700 | 0.28 | 100 | 0.4 | 0.112 |

Fig. 4. Selecting relay node according to its relay score

chosen for relay and thus it will die quickly. In this case, the energy utilization is unbalanced. So, we apply the energy-proportional principle [2][3] and consider the relay node's *remaining energy* (E_R). Actually, in the relay region we consider the respective proportions of each node's E_S and E_R in the total E_S and total E_R . The proportions are called node's *SE-Ratio* and *RE-Ratio* respectively. Finally, we get *Relay_Score* as the product of *SE-Ratio* and *RE-Ratio*, and pick the node has the maximum *Relay_Score* to join the routing path and to relay data in the traffic. Fig. 4 illustrates that EGR determines node B as the relay node in the traffic.

3.2 Ad-Hoc Routing with Location Information

The proposed EGR can be easily combined with any geographic routing algorithm. We illustrate AODV [5] and DSDV [11] as examples adopting EGR because AODV and DSDV are the most commonly used routing protocol in mobile ad-hoc wireless networks.

AODV [5] finds a multi-hop routing path between a pair of source and destination, and EGR works for each one-hop link over the routing path. Because AODV is not a geographical routing algorithm, we modify route request (RREQ) to satisfy EGR constraint (3). The modified AODV flow chart is illustrated in Fig. 5 (a). When source wants to find destination in the network, it broadcasts RREQ to search. Because EGR needs neighbors' location information to calculate each E_S , we attach sender's location information to RREQ packet and every node certainly caches its one-hop neighbors' location information. EGR gets neighbors' remaining energy in the same way and this leads to few control overheads. When destination receives the first RREQ packet, AODV back traverse the routing table and sends route reply (RREP) to route node until source receives RRPL. The proposed EGR is used in each one-hop communication and chooses an optimum relay node according to relay node's E_S and E_R .

DSDV [11] is based on table-driven routing algorithm. Each node maintains a routing table for recording the shortest paths to others nodes within the network. DSDV regards the numbers of hop as the distance and uses Bellman Ford Algorithm to find every routing path. When any routing table is changed or the set update time is up, the network will run DSDV again and all routing tables will be updated. To sum up, EGR can improve most ad-hoc routing algorithms no matter table-lookup driven or not.

We show how table-driven and on-demand ad-hoc algorithms are improved. For DSDV, the embedding of EGR into DSDV flowchart is as shown as Fig5 (b). Each of the traditional DSDV nodes has a routing table. Regarding itself as source and all the others as destinations, a node in DSDV records and updates the shortest distances (in number of hops) to all the destinations using the Bellman-Ford algorithm. The application of EGR is after Bellman-Ford algorithm execution to check each one-hop link whether or not requires relay node. If the relay node exists, update the routing table and broadcast the update information to make other nodes also update. If network topology does not change frequently, such manner can effectively improve the energy utilization.

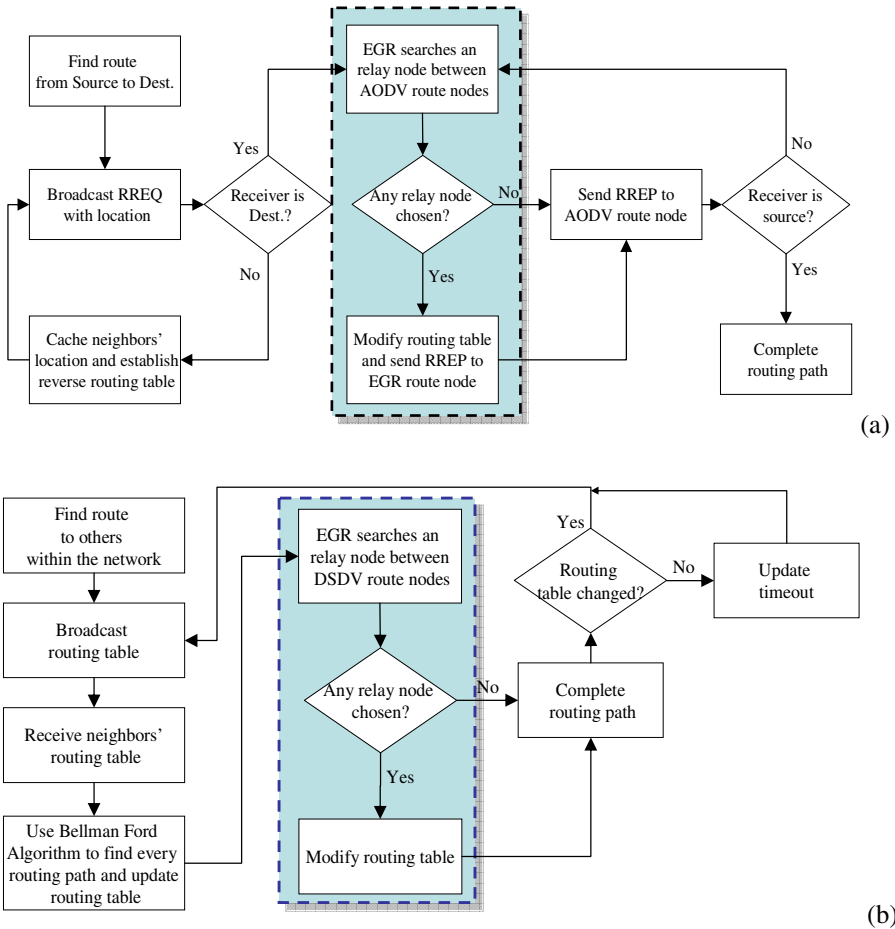


Fig. 5. Flow charts of (a) modified AODV (b) modified DSDV adopting EGR

3.3 Generic Sleeping Scheduler

In addition to path construction, the EGR uses a generic sleeping scheduler in geographical routing. Being applicable to generic scenario, EGR does not separate nodes into two classes such as those in GAF [4]. GAF uses 50 transit nodes (nodes running ad-hoc routing) and 10 traffic nodes acting as sources and sinks. The proposed EGR uses the state diagram shown in Fig. 6 for generic ad-hoc routing. When node is a source or a destination, it enters the traffic state and acts the coordinator in the grid. For transmitting the traffic, the nodes stay in the traffic state until the traffic ends. When traffic is off, all nodes follow the same GAF sleeping scheduling.

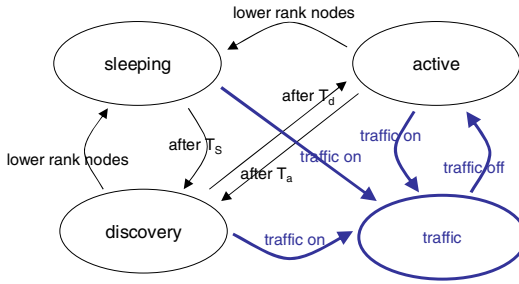


Fig. 6. Sleeping scheduler state diagram of EGR

4 Simulation and Comparisons

EGR highlights the decreasing of energy consumption by adding appropriate relay nodes in original routing path. We perform experiments to show the performance enhancement adopting EGR. The results of numerical analysis show performance comparison with AODV and we use network simulator NS2 [9] for simulations in comparing with GAF. In NS2, d_{max} is 250m as default. The energy consumption of transmit is 1.6W, receiving is 1.2W and idle is 1W.

4.1 EGR Energy Saving

We discuss the comparison in a one-hop link. Considering energy consumption per bit transmission, we perform the experiment showing how a wireless link conserves energy when using EGR. Traditional ad-hoc routing algorithms, such as AODV [5] and DSDV [11], transmit data in the link according to the maximum communication range of the sending node. Assume that the max communication range of each node is d_{max} meters and the source is d_{max} meters apart from the destination. Rather than always using transmission power for sending 1-bit across d_{max} distance, EGR adds a relay node for each one-hop link in the routing path and uses lower transmission power to decrease total energy consumption. In the relay region, different relay node causes different energy consumption. To illustrate the power saving ability of EGR, for each link with different d_{max} , we construct an EGR relay region and calculate the average energy consumption. The energy consumption ratio of using EGR over not using EGR (abbreviated as non-EGR) is shown in Fig. 7. The amplifier parameter values in Section II, we find that energy consumption EGR is the same as non-EGR within 45m and the relay region exists beyond 45m. EGR is slightly superior to non-EGR when d_{max} is between 45m and 87.7m if using FS model. EGR achieves maximum performance over non-EGR when d_{max} is about 230m and it promotes about 60% energy utilization. Note that the experiment is applied to when a relay region has a relay node. When there is no suitable relay node in the relay region, the energy consumption for the link is the same as that in non-EGR.

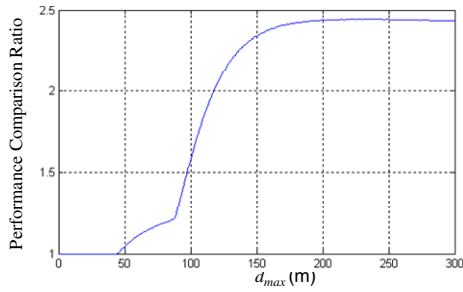


Fig. 7. The energy consumption ratio of non-EGR to EGR with various d_{max}

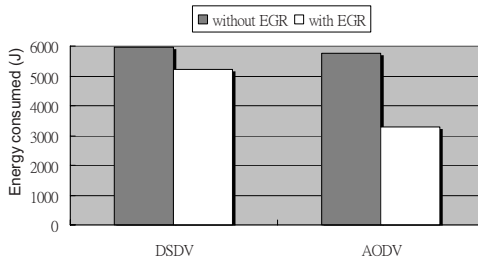


Fig. 8. Comparison of the energy consumption between DSDV, AODV and EGR

In other way, we use NS2 to simulate EGR energy saving. Considering the energy consumption for transmission, we assume 50 motionless nodes with infinite energy forming a small-scale network in a 1500x300 m² area and random traffic lasts whole simulation time (900 seconds). The traffic generation randomly chooses two nodes as source and destination with 0.1s packet interval. The traffic generation appears every 100s until end of simulation. We compare EGR to both AODV and DSDV with average energy consumption of ten times of simulations. Fig. 8 shows EGR can promote about 43% energy efficient over AODV and about 12% over DSDV. Because in DSDV, frequent broadcasting of update information is required, energy saving becomes smaller.

4.2 Enhancing Energy Utilization and Lifetime in GAF

Routing with traditional AODV, traffic in GAF could not satisfy the relay inequality (3). We measure network lifetime by the fraction of all nodes with non-zero energy as a function of time [4]. In the simulation, three mobility situations – pause-times 30s, 300s and 900s are assumed and all nodes have the same movement speed (20m/s). Nodes pause and then move to randomly chosen locations at 20m/s speed. The total simulation time is 900s and we regard the case of pause-time 900s as that all nodes don't move while we regard the 30s-pause-time case as in high mobility. The same in GAF [4], we also use constant bit rate (CBR) traffic with packet length 512-bytes and packet rate 10 pkts/s. Using more generic ad-hoc wireless network scenario that all nodes evenly possess the same initial energy of 450 joules. Fig. 9 shows the results of

the simulation. EGR sends more packets than GAF due to the nodes in GAF waste more energy in transmitting data if equation (3) is not met. GAF source nodes die more quickly and eventually fewer packets are sent. Furthermore, in the whole 900s simulation the average energy consumption of EGR is lower than of GAF. Therefore, EGR has higher energy utilization and shown in Fig. 10 it extends the network lifetime no matter what the pause-time is.

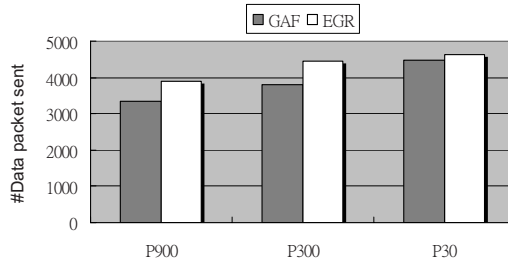


Fig. 9. Data delivery comparisons to GAF in cases of different pause times

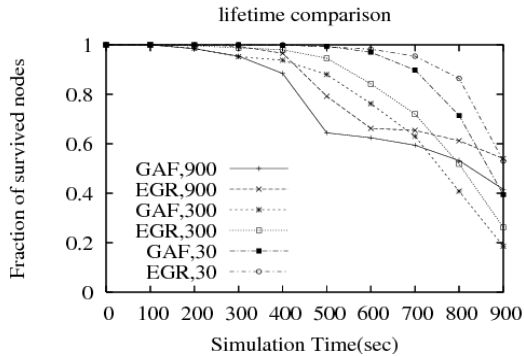


Fig. 10. Simulation results of GAF and EGR for network lifetime with different pause times at high node speed (20m/s)

5 Conclusion

We have found a new relay mechanism and developed a routing protocol called EGR to improve energy utilization in wireless communication networks. Derived from the relay inequality, we get the relay region to ensure each one-hop link is energy-efficient in a routing path. No matter on-demand protocols such as AODV or table-lookup driven protocols such as DSDV are enhanced by EGR with better energy efficiency and load balance. Furthermore, EGR can be applied to any geographical routing protocol by improving energy consumption of each one-hop link. We compare the performance of two GAF versions of using and not using EGR. The one using EGR consumes lower energy per data unit. With energy efficiency and load

balance, EGR prolongs networks lifetime. Future works include the adaptive relay region in the different environments considering more complicated and correlated radio models such as shadowing and fading.

Acknowledgement

The authors would like to thank the National Science Council in Taiwan R.O.C for supporting this research, which is part of the three projects numbered NSC 95-2221-E-168-029, NSC 95-2221-E-006-289-MY2 and NSC 95-2221-E-006-371.

References

1. European Radiocommunications Office. ERC/DEC(99)23, <http://www.ero.dk/doc98/Official/Pdf/DEC9923E.PDF>
2. Chen, C.-L., Lee, K.-R.: An Energy-proportional Routing Algorithm for Lifetime Extension of Clustering-based Wireless Sensor Networks. *Journal of pervasive computing* (2) (2006)
3. Chen, C.-L., Lee, K.-R.: An Energy-proportional Routing Algorithm for Lifetime Extension of Clustering-based Wireless Sensor Networks. In: *Proc. The 2nd Workshop on Wireless, Ad Hoc, and Sensor Networks, Taiwan* (2006), <http://acnlab.csie.ncu.edu.tw/wasn06/>
4. Xu, Y., Heidemann, J., Estrin, D.: Geography-informed energy conservation for ad hoc routing. In: *Proceedings of 7th Annual International Conference Mobile Computing and Networking*, pp. 70–84 (2001)
5. Perkins, C., Royer, E.M.: Ad hoc on demand distance vector (AODV) routing. In: *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100 (1999)
6. Ko, Y.-B., Vaidya, N.: Location-aided routing (LAR). in mobile ad hoc networks. In: *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 66–75 (1998)
7. Chen, B., Jamieson, K., Balakrishnan, H., Morris, R.: Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. *ACM Wireless Networks Journal* 8(5), 481–494 (2002)
8. Yu, Y., Govindan, R., Estrin, D.: Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks. UCLA Computer Science Dept., Technical Report UCLA/CSD-TR-01-0023 (May 2001), <http://cens.cs.ucla.edu/Estrin>
9. The VINT Project. The ns manual, <http://www.isi.edu/nsnam/ns/>
10. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-efficient routing protocols for wireless microsensor networks. In: *HICSS. Proc. 33rd Hawaii Int. Conf. System Sciences* (January 2000)
11. Perkins, C.E., Bhagwat, Pravin: Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In: *Proceedings of 1994 ACM SIGCOMM 1994*, pp. 234–244 (August 1994)

Description of a New Feature Meta-model

Yu Song and Qi Chen

School of Computer Science and Technology, North China Electric Power University,
Bao Ding, He Bei
chenqi19820417@163.com

Abstract. At present, several feature meta-models have been come up with. However, they can't meet the requirements of dynamic Internet environment or software reuse. This paper proposes a feature meta-model based on ontology as well as its formal description. Meanwhile, FTM (Flexible Transaction Model) mechanism is considered. In particular, it is adaptable to the changes in dynamic environment and can meet the requirement of software reuse. Finally, an example is given to verify this model.

1 Introduction

Feature model was introduced from the Feature-Oriented Domain Analysis (FODA) methodology [Kang et al.1990] and further developed from a number of approaches^[1-3]. Since its introduction in 1990, feature modeling has attracted a great number of application domains. And it becomes the most popular method of domain analysis with the development of domain engineering and product line. In addition, a large number of tools supporting the feature modeling paradigm have been come up with. However, feature modeling still has not made its break-through into the toolbox of every software architecture or requirement engineering. What's more, in most feature-oriented methods, the construction of feature models heavily depends on the domain analysts' personal understanding, and the work of constructing feature model from the original requirements of sample applications is often tedious and ineffective. So it is necessary to build a common meta-model without misunderstanding.

According to above requirements, this paper proposes a new feature meta-model to adapt to the dynamic network. It divides feature into *Business Action*, *Facet*, *Term*, etc. on the basis of the traditional feature modeling methods[4]. Considering FTM mechanism, it introduces ontology as a descriptive method and take commonality, variability, dependency and bindtime into account comprehensively. With the proposed meta-model, good-quality feature models can be constructed in a more effective way.

The remainder of this paper is organized as follows. Section 2 introduces FTM mechanism. In section 3, we describe the feature meta-model based on FTM and ontology in an all-around way, including the formal descriptions. Section 4 put it into practice in a real system, while conclusions and an outline for further work round up the paper are referred in Section 5.

2 FTM Mechanism

The goal of FTM is to make systems adapt to dynamic transactions, and its application to Supply Chain Management was given by JUN AHN and JOO PARK several years ago. To make the goal clear, we define a transaction as a “collaborative process of exchanging information for trading goods or performing trade-related activities”[5]. This definition is different from that of traditional transaction processing literature, i.e., ACID(Atomicity, Consistency, Isolation, and Durability) which is emphasized for maintaining data integrity[6-7].

Under today’s complicated and changeful network environment, FTM mechanism should be paid more attention in building software models.

3 Optimized Feature Meta-model

3.1 Ontology

A commonly accepted definition of an ontology in information science and engineering is that by Gruber, who defines an ontology as “an explicit specification of conceptualization”[8]. An ontology represents the semantics of concepts and their relationships using some description language, which is most often coupled with first-order logic or its decidable fragment. In terms of descriptive power, ontology is clearly richer and more powerful than feature, which is the reason why we combine them together to make a more powerful feature meta-model.

3.2 Feature Meta-model

Feature model is a hierarchical structure with constraint relations between features and is originally developed from customers’ point of view. It is also a concept description technique, but is captured logically as a propositional formula[9]. The essence of a feature model is its embodiment of hierarchy and description of variability, rather than its rendering. Each feature can be optional or mandatory for a set of systems within a domain. Figure 1 shows an example of a simple feature model.

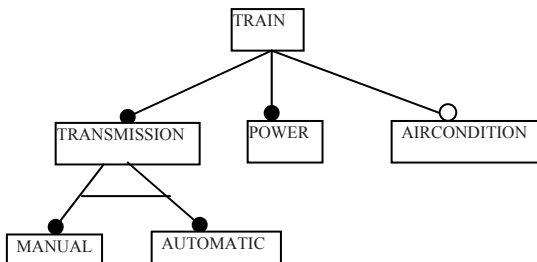


Fig. 1. Train Feature Model

In this figure, *AIRCONDITION* is an optional feature, while the other two features are mandatory. In addition, *MANUAL* and *AUTOMATIC* are exclusive with each other.

The ideas of modeling and expressing relations presented in FODA (Feature Oriented Domain Analysis) are further developed in FORM (Feature-Oriented Reuse Method) [Kang et al. 1998]. FORM extends FODA to the software design and implementation phases and describes how the feature model is used to develop domain architectures and components for reuse, such as attributes and cloning, which seem to be pushing the descriptive power of feature modeling to that of ontology [10]. However, it is difficult to use the FORM feature views because their separation is not defined precisely enough. Furthermore, reverse engineering needs a more general separation of the feature spaces. So we apply ontology to feature meta-modeling to make a more powerful description method, taking FTM mechanism into consideration.

3.3 Description of Meta-model Based on FTM and Ontology

Research on features has received much attention in the domain engineering community. Feature modeling plays an important role in the design and implementation of complex software systems. However, the presentation and analysis of feature models are still largely informal. There is also an increasing need for methods and tools that can support automated feature model analysis. A formal semantics for the feature modeling language is defined using first-order logic. It provides a precise and rigorous formal interpretation for the graphical notation. The proposed feature meta-model is shown in figure 2. We use OWL to describe it. It further divides feature into *Business Action*, *Facet*, *Term*, etc. on the basis of the traditional feature modeling methods. The model is denoted by ontologies and can be commonly used for applications in every domain. Considering FTM mechanism, we add several dynamic or changeable elements to this model, such as *Bind*, *ConfigureDepend*, *HasChildren*, *IfOptional*, etc. They are not necessary for every system, but I want to describe the meta-model as integrately as possible, so I add these elements to it for the utilization in some cases.

The meta-model consists of four ontology classes which are *BusinessAction*, *BusinessObject*, *Term* and *Bind Time*. Also, it includes several relations, and some relations are defined on the basis of other relations.

We divide the meta-model into two parts. The upper one which is in the dashed rectangle is commonly used. We abstract it from the complicated meta-model in order to achieve the purpose of software reuse and make a clear vision to developers and designers of software products. The nether one are dynamic and not every element in this part is necessarily be used in a certain system. Therefore, it is comprehensive and can adapt to the dynamic system environment. In this model:

BusinessAction is the semantic agent in the course of exchanging information.

Term is the terminology value of *Facet*.

They build themselves into a hierarchical structure respectively according to the relation *Subclassof*, and show the specialized relation between *BusinessAction* and *Term*.

Facet gives a precise description of *BusinessAction* in detail. It is defined as the relation from *BusinessAction*(*rdfs:domain*) to *Term*(*rdfs:range*).

ConfigureDepend stands for dependences under indirect communication situation. It signifies mutual constraint relationship when the optional features are binded.

Subclassof is defined between *BusinessAction* and *Term*. It signifies direct specialized relations which can be converted into the relation *subClassof* in ontology(*rdfs:subClassof*), and remain direct *subClassof* relation.

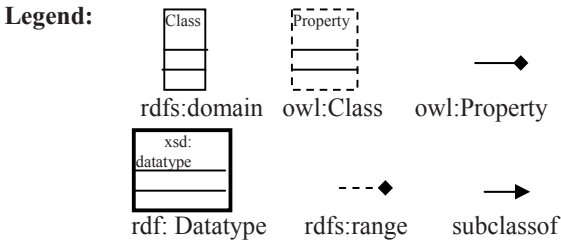
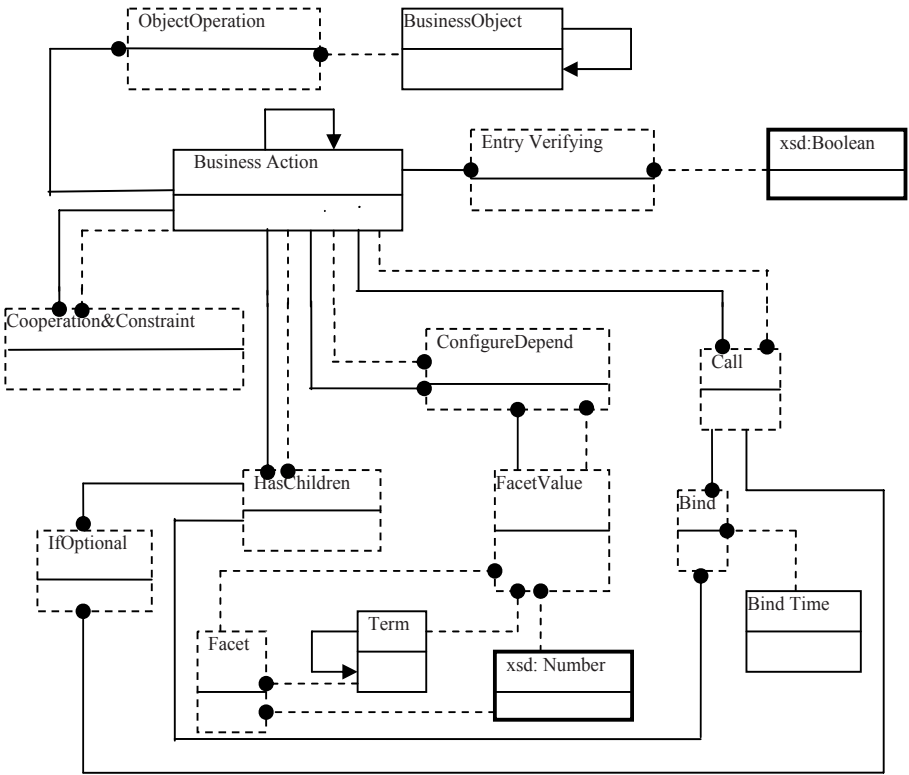


Fig. 2. Feature Meta-model Based on FTM and Ontology

HasChildren shows the division of the parent action.

Call stands for the dependency to other operations in order to achieve current function.

IfOptional symbolizes whether a *BusinessAction* is optional or not.

Cooperation&Constraint defines the relations among *BusinessActions*, such as notice, decision, etc.

Bind describes the constraints when the optional or variable elements are related to their above *BusinessAction* or *Use*. It has three types, i.e., BuildTime, LoadTime and RunTime which are used in system assembly, guidance and operation time respectively.

HasChildren is another relationship between *BusinessActions*, the parent BusinessAction is related to a set of sub-BusinessActions according to this relationship.

3.4 Formal Semantics for the Feature Meta-model

In this section, we propose a formal semantics based on the first-order logic of Z to describe the feature meta-model. The feature types can be expressed precisely through these descriptions[11].

Features represent distinguishable characteristics of a concept, while a concept consists of a set of related features with constraints. We give the definitions of Feature and Concept as follows.

[Feature] | Concept: \mathbf{P} Feature

We define *Feature* as a given set, and *Concept* a special kind of feature, which is represented as subset of *Feature*.

holds: $\text{Concept} \leftrightarrow \text{Feature}$

$\forall c: \text{Concept} \bullet (c, f) \in \text{holds}$

The above defines the relationship *holds* between a concept and the feature of concept instance. This is the most basic and general relationship in a feature model. Then some of the formal descriptions of the relations in figure 2 are defined as follows:

- *IfOptional*

If the result is true, that means the feature is optional. It can be defined formally as follows:

Optional: $\text{Concept} \leftrightarrow (\text{Feature} \times \mathbf{P} \text{Feature})$

$\forall c: \text{Concept}; pf: \text{Feature}; s: \mathbf{P} \text{Feature} \bullet c \text{ Optional}(pf, s) \Leftrightarrow pf \notin s$

$\wedge ((c, pf) \notin \text{holds} \Rightarrow (\forall f: s \bullet (c, f) \notin \text{holds}))$

The first predicate states that the parent feature *pf* should not be included in the child set *s*. The second predicate states that if the parent feature *pf* of a set of *Optional* features *s* is not included in a feature configuration, none of the set *s* can be included in the same concept instance.

On the contrary, if the result is false, the feature will be mandatory:

Mandatory: $\text{Concept} \leftrightarrow (\text{Feature} \times \mathbf{P} \text{Feature})$

$\forall c: \text{Concept}; pf: \text{Feature}; s: \mathbf{P} \text{Feature} \bullet c \text{ Mandatory}(pf, s) \Leftrightarrow pf \in s$

$\wedge ((c, pf) \in \text{holds} \Rightarrow (\forall f: s \bullet (c, f) \in \text{holds}))$

$$\wedge((c, pf) \notin \text{holds} \Rightarrow (\forall f: s \bullet (c, f) \notin \text{holds}))$$

The above defines *Mandatory* as a relation between a concept c and the parent and children of feature f . It states that if the parent of the *Mandatory* feature set s is held by a concept instance, all the feature in set s should be included into the description of the same concept instance; otherwise none.

- *HasChildren*

HasChildren: Concept \leftrightarrow (*Feature* \times *P Feature*)

$$\forall c:\text{Concept}; pf:\text{Feature}; s:\mathbf{P Feature} \bullet c \text{ HasChildren } (pf, s) \Leftrightarrow pf \in s$$

$$\wedge((c, pf) \in \text{holds} \Rightarrow (\exists f: s \bullet (c, f) \in \text{holds}))$$

$$\wedge((c, pf) \notin \text{holds} \Rightarrow (\forall f: s \bullet (c, f) \notin \text{holds}))$$

The above predicate suggests if the parent feature of set s is held by a concept instance, there must be at least one child which is included into the description of the same concept instance; otherwise none.

4 Application of This Model

4.1 Online Auction Management System

The advancement of Internet-based commerce has created a turbulent market environment by allowing easier introduction of new products, services, and suppliers. The time and efforts required to open new storefronts on Internet became much smaller comparing with those of traditional offline markets and various types of business models and marketing practices are newly created due to the constant development of new information technologies [12-14]. For this dynamic environment, information systems need to be designed in a flexible way to meet the changing requirements. This turbulent market environment requires strong adaptability in information systems to avoid high cost for re-implementation or re-customization. So we apply the above feature meta-model to this field to provide an improved and understanding example which can meet all the requirements referred above.

4.2 Description of the Domain Model

The description of the application of feature meta-model in Online Auction System is shown in figure 3. We can see that every kind of symbol in this graph signifies a relationship existing in the above meta-model.

OnlineAuction mainly includes the mandatory *Sailing*, *Purchasing* and *OrderPayment*, and also the optional *Delivery*.

PayWhenReceive means pay the cash to deliveryman when the consumers receive their goods. This is an optional item.

The flexibility is reflected on the dynamic dependence of *BidMateria*, *DelObtainedMaterial* and *Delivery* towards their parent BusinessActions.

Two facets are defined on Browse, i.e., *BrowseTime* and *BrowseMode*. Three types of *BrowseMode* also provide an optional operation to the customers.

PayToBank has three subclasses, i.e., *CCB*, *CMB* and *ICBC*. The customers can select different ways of payment at the time of system running, which shows the flexibility of design again.

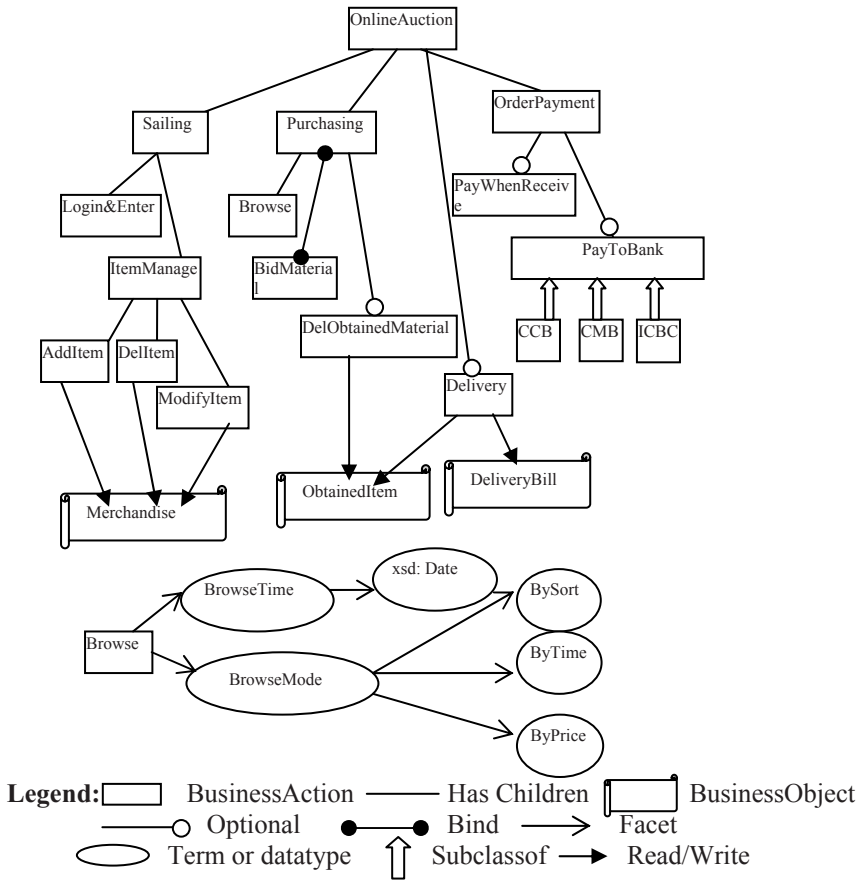


Fig. 3. Application of Feature Meta-model

5 Conclusions

We put forward a feature meta-model based on FTM mechanism and ontology and then apply it into Online Auction Management System and we have proved that it has the greatest descriptive power and the biggest adaptability to dynamic network than any traditional method. In particular, we give out formal descriptions of this model in details. However, there are still some works which need to be perfected, such as how to make the meta-model simpler and clearer and the improvement of formal description of this meta-model. Therefore, we should study further and apply the model to applications as possible as we can.

Acknowledgements

I acknowledge for the help of my tutor during my preparation for the paper.

References

1. Griss, M., Favaro, J., dAlessandro, M.: Integrating feature modeling with the rseb. In: *Proceedings of the Fifth International Conference on Software Reuse*, pp. 76–85. IEEE Computer Society Press, Victoria, Canada (1998), see <http://www.intecs.it>
2. Kamiya, T., Kusumoto, S., Inoue, K.: Cnder: A multi-linguistic token-based code clone detection system for large scale source code. *IEEE Trans. Software Engineering* 28, 654–670 (2002)
3. Riebisch, M., Boellert, K., Streitferdt, D., Philippow, I.: Extending feature diagrams with uml multiplicities. In: *IDPT 2002. Proceedings of the Integrated Design and Process Technology*, pp. 1–7 (2002)
4. Zhang, W., Mei, H.: A feature-oriented domain model and its modeling process. *Journal of Software (in Chinese with English abstract)* 14(8), 1345–1356 (2003), <http://www.jos.org.cn/1000-9825/14/1345.htm>
5. Ahn, H.J., Park, S.J.: A flexible transaction framework for dynamic collaboration of agents—with an online travel application. *International Journal of Cooperative Information Systems* 13(4) (2004)
6. Gray, J., Reuter, A.: *Transaction Processing: Concepts and Techniques*, pp. 5–7. Morgan Kaufmann Publishers, San Francisco (1993)
7. Jajodia, S., Kerschberg, L.: *Advanced Transaction Models and Architectures*, pp. 3–34. Kluwer Academic Publishers, Dordrecht (1997)
8. Gruber, T.R.: Towards principles for the design of ontologies used for knowledge sharing. Technical Report KSL93-04, Stanford University, Stanford (August 1993)
9. Batory, D.: Feature models, grammars, and propositional formulas. Technical Report TR-05-14, University of Texas at Austin, Texas (March 2005)
10. Czarnecki, K., Kim, C.H.P., Kalleberg, K.T.: *Feature Models are Views on Ontologies*. IEEE, Los Alamitos (2006)
11. Sun, J., Zhang, H.: *Formal Semantics and Verification for Feature Modeling*. IEEE, Los Alamitos (2005)
12. Jelassi, T., Leenen, S.: An e-commerce sales model for manufacturing companies: A conceptual framework and a European example. *European Management Journal* 21(1), 38–47 (2003)
13. Schlegelmilch, B., Sinkovics, R.: Viewpoint: Marketing in the information age, Can we plan for an unpredictable future? *Int. Marketing Review* 15(3), 162–170 (1998)
14. Yelkur, R., DaCosta, M.: Differential pricing and segmentation on the Internet: The case of hotels. *Management Decision* 39(4), 252–261 (2001)

Studying of Multi-dimensional Based Replica Management in Object Storage System*

Zhipeng Tan **, Dan Feng ***, Fei He, and Ke Zhou

Key Laboratory of Data Storage System, Ministry of Education
School of Computer, Huazhong University of Science and Technology,
Wuhan 430074, Hubei, China
zhipengtan@163.com

Abstract. The Object-based Storage System (OBS) has been proposed as a novel information storage technology in adaptation to the explosive growth in information quantity under the next-generation internet. The OBS treats all storage devices (OSD) and data information as objects, hence, the issues like reducing access delay over WAN, saving limited bandwidth and enhancement of data validity become problems related to the overall performance of OBS. To address these problems, we have the replica-based OBS, which brings forward a new issue on how to manage these replicas. In this paper, we present a multi-dimensional replica management scheme, and study the object searching performance within this mode. We deliver the optimal tree & improved one-path tree on the basis of similarity searching, with detailed replica indexing algorithm and emulation tests. The result of these experiments justifies their better performance in contrast to normal similarity-based indexing algorithm, with lower system cost.

Keywords: Multi-dimensional Architecture, Optimal tree, One-path tree, Replica management, Searching.

1 Introduction

In the last few years, object storage system is a research hotspot and it is the key technology for next generation network storage. In the object storage system, object is the base unit of management. Object storage system provides geographically distributed storage resources for large-scale data-intensive applications that generate large data objects. However, ensuring efficient and fast access to such huge and widely distributed

* It was supported by the National Basic Research Program of China (973 Program) under Grant No. 2004CB318201.

** Corresponding author. Tan Zhipeng is a Ph.D candidate in Department of Computer Science, Huazhong University of Science & Technology. He is interested in computer architecture, information storage and database technology etc..

*** Feng dan is a professor of Huazhong University of Science & Technology. She is interested in computer architecture, mass information storage and disk array etc..

data objects is hindered by the high latencies of the Internet. To address these problems we introduce a set of object replication management services and protocols that offer high data availability, low bandwidth consumption, increased fault tolerance, and improved scalability of the overall system. Replication decisions are made based on a cost model that evaluates data access costs and performance gains of creating each replica. Replication technology is applied in the field of grid, data grid, and distributed system. Although there are some research results about replication, there is no research of replication about object storage system. Our study investigates the usefulness of creating replicas to distributed object among the various nodes in the object storage system. The main aims of using replication are to reduce access latency and bandwidth consumption. Replication can also help in load balancing and can improve availability by creating multiple copies of the same object. Since the numerous replicas are redundantly stored, the number of which soars when the amount of object storage nodes and data objects increase, how to manage these replicas becomes an important problem for object storage system. In the object storage system, one of the simplest rules for managing replicated object is where read operations on an object are allowed to read any replica, and write operations are required to write all copies of the object. The rule is termed as read-one & write-all. In this paper, we provide a multi-dimensional-based replica management to control replicas, and the experiments prove its effectiveness to advance performance of object storage system with replication.

The rest of the paper is organized as follows: First, we will give related work in the Section 2; then delivers a Multi-dimensional replica management model of object storage system in section 3; section 4 discusses the implementation of multi-dimensional replica management model; in section 5, the performance of the Multi-dimensional replica management model is analyzed in terms of object availability. At last, we will conclude in section 6.

2 Related Work

Replication has been studied extensively and various distributed replica management strategies have been proposed in the literatures^[1, 2, 3]. In the context of object storage technology, replication is mostly used to reduce access latency and bandwidth consumption. But replication will bring large numbers of replicas on the object storage system. Consequently, it is an important matter that how these replicas are managed. There are some researches about the size of the object replication in the grid^[8], the placement of object replicas and the selection of consistency algorithms. The replica management system decides when to create and where to place a replica. These decisions are made based on a cost model that evaluates the maintenance cost and access performance gains from creating each replica. The estimates of costs and gains are influenced by many factors, such as run-time accumulated read/write statistics, the chosen consistency algorithm, run-time measured network latency, response time, bandwidth, and replica's size^[8]. These parameters are changing during the program

execution, so they need to be measured at runtime and fed to an optimization procedure that minimizes object access costs by dynamically changing the replicas number and placement.

To ensure scalability, we use both hierarchical and flat propagation graphs spanning the overall set of replicas to overlay replicas on the object storage system and minimize inter-replica communication costs. For the hierarchical topology, we introduce a modified fat-tree structure with redundant interconnections connecting its nodes; closer the node is to the root, more interconnections it has. The fat-tree was originally introduced by Leiserson^[12] to improve the performance of interconnection networks in parallel computing systems. The hierarchical distribution is well suited for multi-tier applications, while the ring topology suits best for the multiple server or peer replica applications. For our flat topology we use the ring one. In the peer-to-peer model, any replica can synchronize with any other replica, and any update can be applied at any accessible replica. The peer model has been implemented in many systems such as Ficus^[1], Rumor^[2], Roam^[6], Bayou^[7], and Locus^[12]. In the hierarchical model, the replicas are placed at different levels, and communicate with each other in a client-server like scheme. This model has been realized in replication systems such as Coda^[10]. To further exploit the properties of both topologies, we use a hybrid topology in which both the ring and fat-tree replica organizations can be combined into multi level hierarchies. This approach improves both the data availability and the reliability of the ring topology and allows for a scalable expansion of the hierarchical distribution. Both the ring and fat-tree connection graphs represent virtual connections between the grid nodes that hold replicas of the same object. Depending on the topology, each node is aware of its neighbors or direct ancestors and children.

As stated above there is no detailed study of management for object replications, which provides an interesting field for exploitation, and in this paper we study the management of object replications specially and analyze performance of object storage with replications. Multi-dimensional-based Replica Management Mechanism should be propitious to find the replication object. First, the replications are placed according to the multi-dimensional replica management model, but when the searching of replication, the structure of multi-dimensional can be transformed structure of tree. The transform is easy. The experiment proved this way is effective for replication management.

3 Multi-dimensional Replica Management Model

In object storage system, there are attributes and operations of object defined, which are judged as two dimensions, while at the same time, we can add more characteristic dimensions to every object, so a Multi-dimensional data structure of replicas can be given according to these attributes. Within three Multi-dimensional data structure, replicas are logically organized into a box with four planes. Figure 1 is an example of the box that consists of four planes with the black circle represents a copy at location A, B, C, ..., and X. The Multi-dimensional data structure restricts the number of replicas in each plane, i.e., if l denotes the length (column) of the plane, and w is the width (row) of the plane, then each plane consists $l \times w$ replicas. Of course we can get new box from other dimensional data structure, the box must not have four planes only.

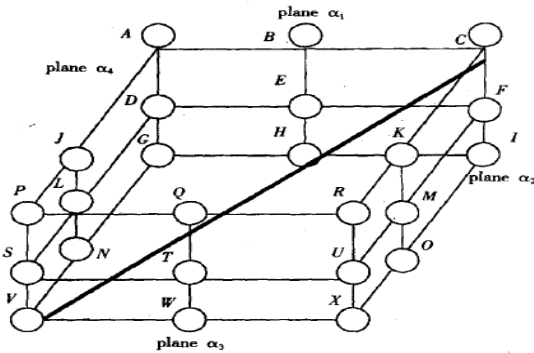


Fig. 1. A box of replicas by three Multi-dimensional data structure

Definition 1. A pair of replicas that can be constructed from a hypotenuse edge in a box-shape structure are called hypotenuse replicas. For the Multi-dimensional replication management structure, reading operations on a replication object are executed by acquiring a read quorum that consists of any hypotenuse replicas. In the Figure1, replicas {V,C},{I,P},{X,A}, or {G,R} are hypotenuse replicas from which it is sufficient to execute a read operation. Since each pair of them is hypotenuse replicas, read operation can be executed if one of them is accessible. If W is a set of write quorums which consists of groups that are sufficient to execute write operations under a set of hypotenuse replicas, say {V,C}, then from Figure 1, we have

$$W = \{ \{V,C,I,A,G,B\}, \{V,C,I,A,G,E\}, \{V,C,I,A,G,H\}, \{V,C,I,R,X,K\}, \{V,C,I,R,X,M\}, \{V,C,I,R,X,O\}, \{C,V,P,A,G,J\}, \{C,V,P,A,G,I\}, \{C,V,P,A,G,N\}, \{C,V,P,R,X,Q\}, \{C,V,P,R,X,T\}, \{C,V,P,R,X,W\} \}.$$

Of course, there is weakness of the Multi-dimensional replication management structure — that is, if all store nodes in a column of each plane are unavailable, the write quorum can not be constructed. For example, when { {B,E,H}, {K,M,O}, {Q,T,W}, and {J,L,N} } are unavailable, the write operation is suspended even if all the other store nodes are available or accessible. So in this paper, we mainly discuss how to search the replicas needed in object storage system that has plentiful amount of object replicas by Multi-dimensional replication management structure.

4 Searching of Multi-dimensional-Based Replica Management

Multi-dimensional index technology has been recognized as one of the key solutions to the acceleration of data searching. And there are already numerous hyper-dimensional index methods, for instance, the R-tree^[14], R*-tree^[15] as well as some variations of the R-tree^[14-17], which are all based on space locality, and have been widely used in GIS(Geology Information System). However, these sorts of space locality based index

methods has their innate confinement, which proves only to be effective when the following two conditions are met simultaneously: (1) the indexing object must be able to be denoted by a Eigen-value of hyper-vector space; (2) the similarity between objects must be measured by the Euclid Distance. As for the need of quick replica searching in the Object Storage System(OBS) grounded on replicas, we first institute a measurement of space through multi-dimensional replica management, and then elicit the distance-based index theory. Unlike the locality-based index technology, the distance-based one mainly deals with the comparative distance between replicas, without concerning the relative locality between them. As some typical models in this kind, one need to look no further than the M-tree^[17], MVP-tree^[18] and MB+tree^[19], among which the VP-tree and MVP-tree are two canonical space measurement-based static index architectures, while the M-tree becomes the leading one to realize the dynamic. Additionally, the M-tree model has been improved by MB+tree and Slim-trees, for the MB+tree substitutes the hyper-dimensional index structure by two mono-dimensional index(B+tree & Block-tree) to avoid the overlapping partition of the data space, while the Slim-trees adopt a disposal procedure after creating the tree to minimize the total number of nodes and the cover radius of the data node. Nevertheless, the searching performances of these distance-based index technologies are primarily depended on the specific data distribution, and most of which includes some empirical parameters to design the models(the vantage points in VP-tree, for example), far from the “Optimal Searching Performance”. For this reason, with the idea of multi-dimensional replica storage structure under the object storage space, we introduce a brand new distance-based theory of index structure, the optimal tree and the improved one-path tree, by studying their establishment and detailed accomplishment of searching, with corresponding algorithms.

4.1 Similarity Searching

We first define the OBS’s storage space as a binary group: $M=(D, d)$, in which D is the characteristic space of the object, and d is the length measurement under the D . They together meet the following conditions:

- ①symmetry: $d(x,y) = d(y,x)$;
- ②non-negative: when $x \neq y$, $0 < d(x,y) < \infty$, when $x = y$, $d(x,y) = 0$;
- ③triangle inequality: $d(x,y) \leq d(x,z) + d(z,y)$.

From this definition, we conclude that we can only use the 3 conditions defined above when forming the index structure in the distance-based object storage space, in contrary to any other assumptions frequently used in Euclid space. Given a OBS, namely S , and the distance measurement in the object characteristic space, namely d , and Q -the accessing object replica, normally we would searching the certifiable replica through the following two ways:

Threshold-value inquiry-Query(Q, t): given a certain threshold value t , all the target replicas I in the S that fit $d(Q, I) \leq t$.

Best-match inquiry-Query(Q, n): possible n candidate replicas that have the closest distance to the accessing replica in the S .

When concerning the similarity searching, we can use the triangle inequality to reduce the times of distance calculation during the Best-match inquiry process to enhance its efficiency. The detailed method can be described as follows:

Assume I as a replica in the S , and $K=\{K_1, K_2, \dots, K_n\}$ is a set of similar replica objects(-call K_i the key object). By using the triangle inequality, we have:

$$d(I, Q) \geq \max_{1 \leq s \leq m} |d(I, K_s) - d(Q, K_s)| \tag{1}$$

From (1) we know that, for a random $s(1 \leq s \leq n)$, we have $d(I, Q) \geq |d(I, K_s) - d(Q, K_s)|$, thus derives a lower bound of the distance between I and Q . Consider a storage system $S=\{I_1, I_2, \dots, I_n\}$ and a very small set of similar replica objects $K=\{K_1, K_2, \dots, K_m\}$. If for any s and t , the distance between I_s and K_t , $d(I_s, K_t)$, has been calculated in advance, then for the similarity searching Query(Q, t), it is only needed to calculate the set $\{d(Q, K_1), d(Q, K_2), \dots, d(Q, K_m)\}$, and it is easy to get the corresponding lower bound of distance by referring to *inequality (1)*. Apparently, if we can prove $d(I_s, Q) > t$, then we can eliminate I_s from the candidate matching set of Q . After this kind of filtration, it is only necessary to compute every remaining object by the linear searching method, and put those that can meet the demand into the searching result set. In this triangle-inequality based similarity searching strategy, we can simply exclude those impossible replica candidates with too long distance from the inquiring replica with the assistance of “distance lower bound”, thus reducing the times of distance calculation in the query. With this searching algorithm, it only takes $m+u$ time of distance calculation(u is the number of leaving objects after filtration) and $O(mn)$ times of simple computation. Obviously, this strategy can save a great deal of distance calculation to promote the efficiency of similarity searching remarkably, as long as the prerequisite $m+u \leq n$ can be met.

4.2 The Partition、Tree Structure and Searching

We begin to discuss the partition of object replica set with the multi-dimensional object replica management structure. As for convenient explanation, we treat the terms “replica”, “the characteristic vector of replica” as well as “object” and “the characteristic vector of object” as the same thing, as far as it would not lead to confusion.

4.2.1 The Optimal Partition of Multi-dimensional Replica Object Set

Definition 2 (Optimal partition). Assume D as a established multi-dimensional replica set, and d as a distance measurement under D . Select two sample point C_1 and C_2 on a random side of the multi-dimensional object replica management structure. Partition set D by these two points into two child set D_1 and D_2 , so that for a random point X aside from C_1 & C_2 , if $d(X, C_1) \leq d(X, C_2)$, then put X into D_1 ; Or else put it into D_2 .

We call it a “Balance Partition” if it fits the condition (1) defined as follow; For any given positive integer $h > 0$, if the partition meets conditions (1) ~ (3), then we call it

“Optimal Partition”, and the relevant point C_1 and C_2 as “Reference Point” to this partition.

- (1) the minimum of $\text{abs}(|D_1|-|D_2|)$, or the least comparative number of the data nodes in D_1 and D_2 , in which $|\bullet|$ is the operator in the calculation of set base number.
- (2) assume $D'_1=\{X|d(X,C_1)-d(X,C_2)\leq 2h \wedge X \in D_2\}$, $D'_2=\{X|d(X,C_2)-d(X,C_1)\leq 2h \wedge X \in D_1\}$, then demand the least number of data nodes in the set $D'_1 \cup D'_2$ by this partition.
- (3) $d(C_1,C_2) > h$.

By implementing general optimal methods, such as imitative annealing idea or heredity algorithm, we can simply apply the “Balance Partition” or “Optimal Partition” to the replica object set. For a given replica object set, we can employ balance partition or optimal partition to divide it recursively, and thus establish a corresponding index structured optimal tree over the multi-dimensional replica object set. The basic thinking of optimal tree index structure is to adopt a balance or optimal method to divide the multi-dimensional replica space set I into two child sets, and recursively divide each child one with the same method, until each child set include and only include the needed accessing replica. So, the optimal tree is of a binary tree structure, representing a recursive process of partitioning the replica object space.

4.2.2 The Algorithm of the Index Structured Optimal Tree Establishment

Assume $I=(O_1,O_2, \dots, O_n)$ is data set including n replica objects, and d is a distance measurement. Then the establishing algorithm of optimal tree can be described as follows:

Input: dataset I

Output: optimal tree V

- (1) if $|I|=0$, then establish a void tree, return.
- (2) else,
 - (2.1) use a balance or optimal partition method to partition dataset I into two child sets: D_l & D_r (the Reference Points are C_1 and C_2 , accordingly), and
 - $D_l=\{O_i \mid d(C_1,O_i)\leq d(C_2,O_i) \wedge O_i \in I\}$,
 - $D_r=\{O_j \mid d(C_2,O_j)\leq d(C_1,O_j) \wedge O_j \in I\}$;
 - (2.2) branch root V with D_l and D_r as the left & right child tree;
 - (2.3) if D_l or D_r is leaf node, then calculate $d(C_i,O_j)$, put it into leaf-node distance array $D_{i|j}$, return.
- (3) treat D_l and D_r recursively by using the algorithm above, forming relevant optimal child tree.

Theorem 1. Assume D as a replica object set, d is a distance measurement under D , and D_1 & D_2 are two child sets derived from balance or optimal partition, both of which are dimension-decreased replica object sets, and C_1 and C_2 are sample points to D_1 & D_2 . Consider similarity inquiry Query (q,t) (q is the demanded inquiring replica, t is the threshold value). We have, if $d(q,C_1)\leq d(q,C_2)$, then if there exists a point $x \in D_2$ to let

$d(x,C_1)-d(x,C_2)\leq 2t$ stand, we must search D_1 and D_2 to execute similarity inquiry $Query(q,t)$; if not exists, the $Query(q,t)$ only needs to search D_1 . Similarly, if $d(q,C_2)\leq d(q,C_1)$, then if there exists a point $x\in D_1$ to let $d(x,C_2)-d(x,C_1)\leq 2t$ stand, we must search D_1 and D_2 to execute similarity inquiry $Query(q,t)$; if not exists, the $Query(q,t)$ only needs to search D_2 .

Prove: In the first circumstance $d(q,C_1)\leq d(q,C_2)$, because d is a distance measurement, and by the definition of it we can conclude the following two inequalities:

$$\begin{aligned} d(q,C_1)+d(C_1,x) &\geq d(q,x), \\ d(q,C_1)+d(q,x) &\geq d(C_1,x), \text{ derivable from the two inequalities.} \\ d(q,C_1) &\geq |d(q,x)-d(C_1,x)|, \end{aligned} \tag{2}$$

$$\text{and } d(q,C_2)\leq |d(q,x)+d(C_2,x)|. \tag{3}$$

From (2),(3) we have, $d^2(q,C_1)\geq [d(q,x)-d(C_1,x)]^2$, and $d^2(q,C_2)\leq [d(q,x)+d(C_2,x)]^2$. According to the assumption condition $d(q,C_1)\leq d(q,C_2)$, we have:

$$\begin{aligned} [d(q,x)-d(C_1,x)]^2 &\leq [d(q,x)+d(C_2,x)]^2, \\ \Rightarrow -2d(q,x)d(C_1,x)+d^2(C_1,x) &\leq 2d(q,x)d(C_2,x)+d^2(C_2,x), \\ \Rightarrow 2d(q,x)[d(C_1,x)+d(C_2,x)] &\geq d^2(C_1,x)-d^2(C_2,x), \\ \Rightarrow d(q,x) &\geq (d(C_1,x)-d(C_2,x))/2. \end{aligned} \tag{4}$$

From (4) we know, if $d(x,C_1)-d(x,C_2)>2t$ exists, then $d(q,x)>t$. That is to say, if there is a random x in D_2 that leads to $d(x,C_1)-d(x,C_2)>2t$, then x could not be a inquiry candidate. Hence, we only need to search D_1 to execute $Query(q,t)$. Or else, if there exists a point $x\in D_2$ leading to $d(x,C_1)-d(x,C_2)\leq 2t$, then we are not sure whether $d(q,x)$ is smaller than the threshold value. In this case, D_1 and D_2 need to be scanned at the same time to execute $Query(q,t)$. Similarly, the conclusion stands in the second circumstance.

Inference 1. Assume the same condition as Theorem 1, then:

(1) When $d(q,C_1)\leq d(q,C_2)$, if $d(q,C_2)-d(q,C_1)\leq 2t$ stands, then we must scan D_1 and D_2 to execute $Query(q,t)$; Or else, we only need to scan D_1 ;

(2) When $d(q,C_2)\leq d(q,C_1)$, if $d(q,C_1)-d(q,C_2)\leq 2t$ stands, then we must scan D_1 and D_2 to execute $Query(q,t)$; Or else, we only need to scan D_2 ;

Prove: In the 1st circumstance $d(q,C_1)\leq d(q,C_2)$, let $d'=d(q,C_2)-d(q,C_1)$, then to any $x\in D_2$, suppose $d(x,C_1)-d(x,C_2)=d>0$ (see Definition 1). By the triangle inequality, we can have:

$$\begin{aligned} d(q,x) &> d(x,C_1)-d(q,C_1), \quad d(q,x) > d(q,C_2)-d(x,C_2), \text{ thus derives,} \\ 2d(q,x) &> [d(x,C_1)-d(x,C_2)]+[d(q,C_2)-d(q,C_1)]=d+d', \end{aligned}$$

To be more concise: $d(q,x)>(d+d')/2$.

- If $d'=d(q,C_2)-d(q,C_1)>2t$, then $d(q,x)>(d+d')/2\geq t+d/2>t$. From this can we conclude, the $x\in D_2$ has been excluded from the candidate matching list of q . According to x 's random nature, $Query(q,t)$ only needs to scan D_1 .
- If $d'=d(q,C_2)-d(q,C_1)\leq 2t$, we can not guarantee $d(q,x)>t$, which means that we must scan D_1 and D_2 to execute $Query(q,t)$. Similarly, the conclusion stands in the 2nd circumstance.

4.2.3 The Searching over Index Structured Optimal Tree

With Inference 1, we can deliver the searching algorithm of optimal tree as follows:

Optimal tree searching algorithm

Input: optimal tree V

Output: searching outcome set *result*

- (1) Select current node;
- (2) If current node is a leaf node, then to each data node P_i in the leaf node,
 - (2.1) Select distance array D_1 and D_2 ;
 - (2.2) If $\max\{|d(q, C_1) - D_{1[i]}|, |d(q, C_2) - D_{2[i]}|\} > t$, then P_i is a non-matching candidate; Or else, compute the $d(q, P_i)$, if $d(q, P_i) \leq t$, then add it into *result*.
 - (2.3) return;
- (3) if current node is a internal node, then
 - (3.1) compute the distance $d(q, C_1)$ and $d(q, C_2)$;
 - (3.2) if $d(q, C_1) \leq d(q, C_2)$, meanwhile $d(q, C_2) - d(q, C_1) \leq 2t$, then recursively scan its left & right child trees; or else, recursively scan the left child tree.
 - (3.3) if $d(q, C_2) \leq d(q, C_1)$, meanwhile $d(q, C_1) - d(q, C_2) \leq 2t$, then recursively scan its left & right child trees; or else, recursively scan the right child tree.

It is easy to discover from the searching algorithm of optimal tree that, the optimal tree, a distance based multi-dimensional space index structure, can really advance the speed of similarity searching, while the query efficiency of which would not decrease noticeably as the dimension grows. However, because the optimal tree is also of binary searching structure, the level of the tree can be considerable to high-capacity dataset, let alone the cost of recursive searching the child ones which may influence the total performance. To better implement the optimal tree strategy, a feasible way is to deduct the height of the tree to fulfill the aim of reducing the computation of distance. Another possible way that may contribute to the improvement is to ensure the one-way down searching during the query process, without the cost of scanning branches back and forth. Theoretically, this could double the overall performance of searching. With this idea in mind, we deliver a modified optimal tree index structure: the one-path tree.

4.2.4 Improved Indexing One-Path Tree

Definition 3 (Redundant Storage). Assume D, D_1, D_2, C_1 and C_2 has use the same definition as Definition 1. Suppose $D'_1 = \{x | d(x, C_1) - d(x, C_2) \leq 2h \wedge x \in D_2\}$, $D'_2 = \{x | d(x, C_2) - d(x, C_1) \leq 2h \wedge x \in D_1\}$, put the data nodes in D'_1 and D'_2 into D_1 and D_2 overlappingly, thus we have two extended subset $\overline{D_1}$ and $\overline{D_2}$, or $\overline{D_1} = D_1 \cup D'_1$, $\overline{D_2} = D_2 \cup D'_2$. We call the partition above "Redundant Storage". In a storage system like replica-based OBS, which contains a large number of replicas, it naturally results in redundant storage. And in the multi-dimensional replica management mechanism, replica objects on sides formed by different dimensions have dissimilar redundancy, while replicas on various sides tend to have less redundancy or they are totally different object's replicas.

It is easy to discover from Def 2 that, we would get two overlapping extended subsets after a redundant segmentation, with their redundancy determined by parameter h and the particular replica distribution. In the terms of redundant storage, we can use the inequality $d(C_1,x)-d(C_2,x)>2h$ or $d(C_2,x)-d(C_1,x)>2h$ to remove those replicas which are too distant to become a matching candidate. Although the method described here are probabilistic, we can still assure its correctness on similarity searching. Thus can we deduce theorem 2.

Theorem 2. Assume $D, D_1, D_2, \bar{D}_1, \bar{D}_2, C_1$ and C_2 has use the same definition as Definition 3. And to any given user Query(q,t), we have $h \geq t$, then it leads to the following: if $d(q,C_1) \leq d(q,C_2)$, then Query(q,t) only need to search \bar{D}_1 ; or else, Query(q,t) only need to search \bar{D}_2 .

Prove: Suppose $d(q,C_1), d(q,C_2)$. From Def 2 we know, in order to prove that “Query (q, t) only need to search \bar{D}_1 ”, the only necessity is to prove that to a any given $x \in D_2$, if $x \notin \bar{D}_1$, then x can not be a matching candidate of q . On the other hand, from Def 3 we acquire that, if $x \notin \bar{D}_1, x \in D_2$, then $d(x,C_1)-d(x,C_2)>2h$. By referring to the proving method of “Inference 1”, we have

$$d(q,x) > (d+d')/2, \text{ } d' \text{ takes the same meaning as in Infer 1).}$$

Thus derives: $d(q,x) > h+d/2 > h \geq t$, thereby, $d(q,x) > t$. So x is not a matching candidate of q , which in another word indicates that it only takes Query(q,t) to scrutinize \bar{D}_1 .

Similarly can we prove, if $d(q,C_2) < d(q,C_1)$, then Query(q,t) only needs to search \bar{D}_2 .

Definition 4 (one-path tree). Assume I as a Image characteristic vector set, select parameter ξ , and utilize some certain optimal partition method in separate the OBS multi-dimensional replica set into two subsets D_L and D_R . Then use redundant storage strategy to extend the two sub ones so that $D_L = D_L \cup D_L', D_R = D_R \cup D_R'$. Use the same recursive partition and disposition regarding every single extended subclass (D_L & D_R), until each of the two includes and only includes the designated number of data nodes or, the subsets are “small enough”. If the replica object subset $D_L(D_R)$ satisfies $D_L' = D_R (D_R' = D_L)$, then $D_L(D_R)$ can be considered small enough. We call this binary tree architecture through replica object space partitioning the one-path tree.

There is immanent similarity between the one-path tree and the optimal one. And according to Theorem 2, the similarity searching based on one-path tree index structure can be relatively simple, which only takes a single path searching along the one-path tree. Consequently the efficiency of tree searching is boosted prominently.

4.2.5 Searching on One-Path Tree

Input: *one-path tree*

Output: searching outcome set *result*

- (1) If current node is a leaf node, then for every data point P_i in the leaf node,
 - (1.1) Select the distance array and store D_1 & D_2 ;
 - (1.2) If $\max\{|d(q,C_1)-D_{1[i]}|, |d(q,C_2)-D_{2[i]}|\} > t$, then P_i is a non-matching candidate(drop it without compute the distance); or else, compute $d(q,P_i)$. If $d(q,P_i) \leq t$, then put it into the *result*.
 - (1.3) return

- (2) if current node is an internal node, then
 - (2.1) if $d(q,C_1) \leq d(q,C_2)$, search the left child tree recursively;
 - (2.2) if $d(q,C_2) < d(q,C_1)$, search the right child tree recursively;

5 Experiment and Evaluation

In the experiment, we mainly focus on the analysis and comparison of replica-based Object Storage System. We use the two indexing structures: the optimal tree and improved one-path tree, to search for replica object, while recording the searching performance, system cost, access delay queue and I/O flow rate corresponding to the variation of the total amount of replicas and the dimensions of replica management.

The three indexing structure, similarity searching, the optimal tree and improved one-path tree, are all realized by the standard C language under the Linux platform. In the experiment, we study the OBS with 100 storage nodes, and 1000 objects inside. To any object under study, the tested numbers of replicas are 10, 20, 30, 40, 50, which are stored in different nodes. We observe the variation in the searching response time and expense of searching under the three architectures, as well as the access queue generated, with an increasing replicas tendency. Additionally, we observe the three

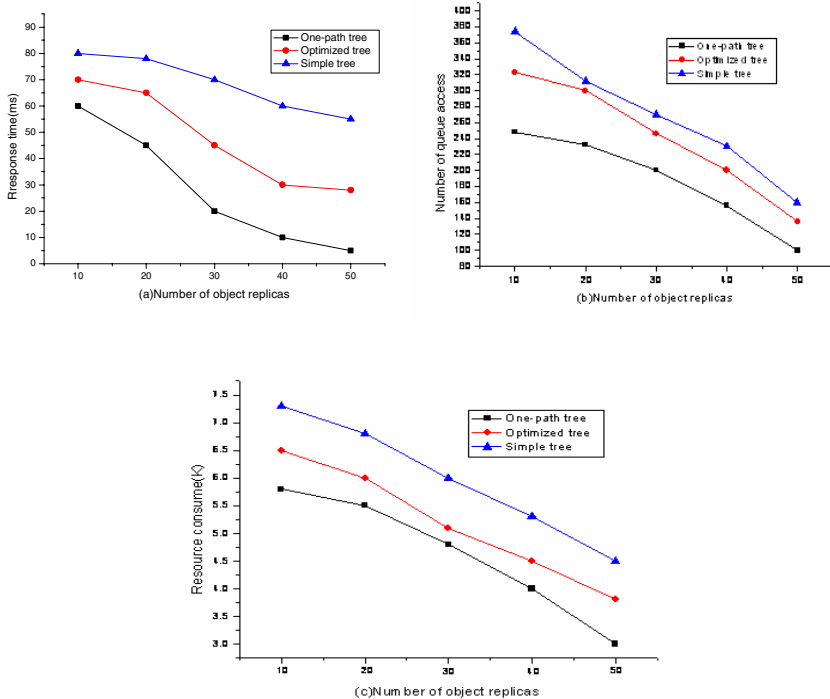


Fig. 2. Influence of Performance by Replicas

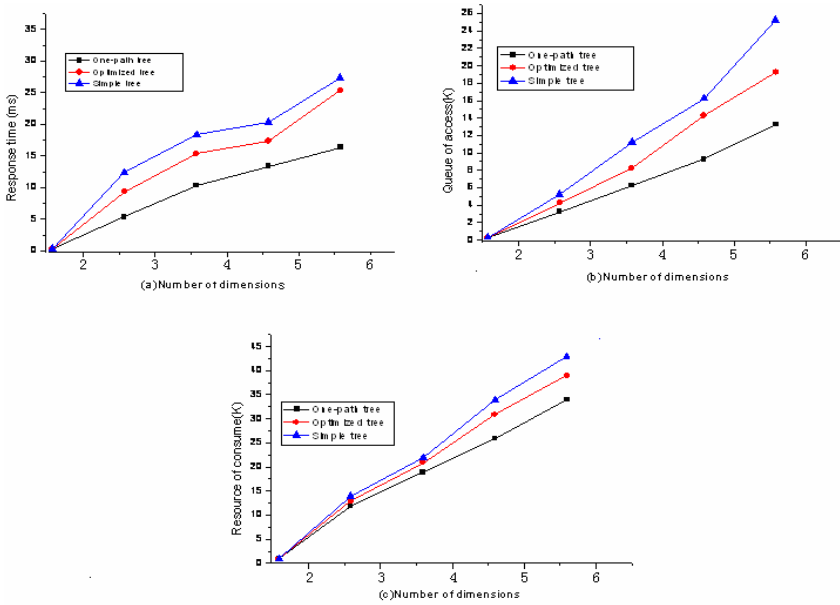


Fig. 3. Influence of Performance by Dimensions

aspects listed above under different replica management dimensions as 2D, 3D, 4D, and 5D. We assume that objects searched are extant object-replicas. The results manifest that the one-path tree has the best searching performance, especially to those queries within a large range.

Figure 2 shows the pattern in the 3 searching architectures: when the object-replica increases, the system response time and system cost drop down, with even shorter waiting queue. It is obvious that the improved one-path tree takes the lead in comparison to the other two.

Figure 3 reveals that when the management dimension increases, the system’s reaction time and its consumption, along with the access queue are all increasing consequently. However, the positive effects the multi-dimensional mechanism plays on replica management are evident, at which we would later be discussed in other special papers. In conclusion, the experiment proves that the performance of improved one-path tree is the best structure in comparison to normal similarity searching and optimal tree.

6 Conclusion

In the object storage system, managing such huge amounts of objects in a centralized manner is almost impossible due to extensively increased data access time. So object replication is a key technique to manage large object in a distributed manner. By its nature, we can achieve better performance (access time) by replicating object in

geographically distributed object stores. In object storage system, user's job may probably require the access to large number of objects, and if the required objects are replicated in the node in which the job is executed, the job is able to process object without any communication delay. However, if required objects are not in the site, they should be fetched from the other nodes. Object fetch takes very long time because the size of a single replica may reach giga-byte scale in some applications while the network bandwidth between nodes is limited. As a result, job execution time becomes lengthy due to delay of fetching replicas over Internet. So searching object is the key factor in replica-based object storage system. In this paper, we advance a model of multi-dimensional based replica management model, and study the searching of object within this model. On the ground of similarity search, we advance optimal tree and improved optimal tree—one-path tree. And the paper gives two kinds of index algorithm under two tree structures, and then tests the algorithm with imitation. At the same time, there are problems emerged on the replicas in the object storage system, such as the placement of replicas、consistency of replicas、granularity of replicas and so on, which would be discussed in other papers.

References

1. Guy, R., Heidmenn, J., Mak, W., Page Jr., T., Popek, G., Rothmeier, D.: Implementation of the Ficus Replicated File system. In: Proceedings of the summer Usenix Conference (1990)
2. Guy, R., Reiher, P., Ratner, D., Gunter, M., Ma, W., Popek, G.: Rumor: Mobile Data Access Through Optimistic Peer-to-Peer Replication. In: Workshop on Mobile Data Access (November 1998)
3. Page, T., Guy, R., Heidemann, J., Ratner, D., Reiher, P., Goel, A., Kuenning, G., Popek, G.: Perspectives on Optimistically Replicated. Peer-To-Peer Filing, Software - Practice and Experience (1997)
4. Ranganathan, K., Foster, I.: Identifying Dynamic Replication Strategies For a High performance Data Grid. In: Proceedings of the International Grid Computing Workshop, Denver (November 2001)
5. Ranganathan, K., Foster, I.: Design and Evaluation of Replication Strategies for a High Performance Data Grid. In: International Conference on Computing in High Energy and Nuclear Physics, Beijing (September 2001)
6. Ratner, D.H.: Roam: A Scalable Replication System for Mobile and Disconnected Computing, PhDThesis, University of California, Los Angeles, Los Angeles, CA (January 1998)
7. Terry, D., Theimer, M., Peterson, K., Demers, A., Spreitzer, M., Hausen, C.: Managing Update Conflicts in Bayou, a Weakly Connected Replicated Storage System. In: Proceedings of the fifteenth Symposium on Operating systems Principles, pp. 49–70. ACM, New York (1983)
8. Vazhkudai, S., Tuecke, S., Foster, I.: Replica Selection in the Globus Data Grid. In: CCGRID 2001. Proceedings of the First IEEE/ACMInternational Conference on Cluster Computing and the Grid, pp. 106–113. IEEE Computer Society Press, Los Alamitos (2001)
9. Wiesmann, M., Pedone, F., Schiper, A., Kemme, B., Alonso, G.: Understanding Replication in Databases and Distributed Systems. In: ICDCS 2000. Proceedings of the 20th International Conference on Distributed Computing Systems (2000)

10. Satyanarayanan, M., Kister, J., Kumar, P., Okasaki, M., Siegel, E., Steere, D.: Coda: A Highly Available File System for a Distributed Workstation Environment. *IEEE Transactions on Computers* 39(4), 447–459 (1990)
11. Popek, G., Walker, B., Chow, J., Edwards, D., Kline, C., Rudisin, G., Thiel, G.: Locus: A Network Transparent High Reliability Distributed System. In: *Proceedings of the Eighth Symposium on Operating Systems Principles*, pp. 169–177. ACM, New York (1981)
12. Leiserson, C.H.: Fat-Trees: Universal Networks for Hardware-Efficient Supercomputing. *IEEE Transactions on Computers* C-34(10), 892–901 (1985)
13. Guttman, A.: R-Trees: A dynamic index structure for spatial searching. In: Yorlmark, B. (ed.) *Proc. of the ACM SIGMOD Conf.*, Boston, pp. 47–57 (1984)
14. Berkman, N., Krigel, H.P., Schneider, R., Seeger, B.: The R*-tree: An efficient and robust access method for points and rectangles. In: Hector, G.M., Jagadish, H.V. (eds.) *Proc. of the ACM SIGMOD Conf.*, Atlantic, pp. 322–331 (1990)
15. Katayama, N., Satoh, S.: The SR-tree: An index structure for high-dimensional nearest neighbor queries. In: Peckham, J. (ed.) *Proc. Of the ACM SIGMOD Conf.*, Tucson, pp. 369–380 (1997)
16. White, D.A, Jain, R.: Similarity indexing with the SS-tree. In: Stanley, Y.W.S. (ed.) *Proc. of the 12th Int'l Conf. on Data Engineering*, New Orleans, pp. 516–523. IEEE Computer Society, Los Alamitos (1996)
17. Ciaccia, P., Patella, M., Zezula, P.: M-tree: An efficient access method for similarity search in metric spaces. In: Jarke, M., Carey, M.J., Dittrich, K.R., Lochovsky, F.H., Loucopoulos, P., Jausfeld, M.A. (eds.) *Proc. of the 23rd VLDB Conf.*, Athens, pp. 426–435. Morgan Kaufmann Publishers, San Francisco (1997)
18. Bozkaya, T., Ozsoyoglu, M.: Distance-Based indexing for high-dimensional metric spaces. In: Peckham, J. (ed.) *Proc. of the ACM SIGMOD Conf. on Management of Data*, Tucson, pp. 357–368 (1997)
19. Ishikawa, M., Chen, H., Furuse, K., Yu, J.X., Ohbo, N.: MB+tree: A dynamically updatable metric index for similarity search. In: Lu, H., Zhou, A. (eds.) *WAIM 2000*. LNCS, vol. 1846, Springer, Heidelberg (2000)

Communication Model Exploration for Distributed Embedded Systems and System Level Interpretations

Takashi Kinoshima, Kazutaka Kobayashi, Nurul Azma Zakaria,
Masahiro Kimura, Noriko Matsumoto, and Norihiko Yoshida

Division of Mathematics, Electronics and Informatics
Saitama University, Saitama 338-8570, Japan
yoshida@ics.saitama-u.ac.jp

Abstract. This paper presents how communication exploration can be done in a design process of distributed embedded systems. Distributed embedded systems involve various communication categories such as event-triggered and time-triggered communication. Therefore, communication exploration is as important as architecture exploration. A design process begins from abstract specification without assuming any communication category, then explores the categories in a stepwise manner, and is followed by physical implementation synthesis. This paper includes system level interpretation of the communication models using the SpecC language so as to verify them.

Keywords: Distributed Embedded Systems, Event-Triggered Communication, Time-Triggered Communication, Stepwise Refinement Design, Model-Driven Architecture.

1 Introduction

Modern embedded systems often work in networks, which comprise *distributed embedded systems*, as found in vehicles for example. Distributed embedded systems involve communication in various layers, from bus connections to networks, thus communication design is more important and difficult than in single embedded systems.

System-Level Design have been gradually used into practice for embedded system design. Its typical design process proceeds as shown in Fig. 1 [1,2]. It is a stepwise refinement process from abstract specification to implementation.

An issue, from the network point of view, in the above process when applied to design of distributed embedded systems is that communication is concerned mainly with bus connections, thus communication exploration is not separated from architecture exploration, in which a suitable combination of modules is explored among several possibilities to fix an architecture model [3].

This paper presents how communication exploration can be done in a design process of distributed embedded systems using an example of event-triggered

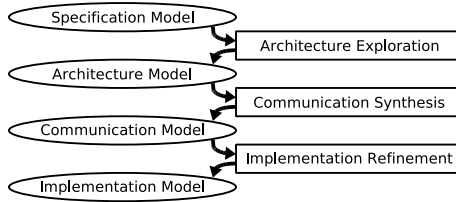


Fig. 1. Design Process for Embedded Systems

and time-triggered communication. This paper also includes system level interpretation of the communication models using the SpecC language so as to verify them. SpecC is used because it is tightly coupled with the above-mentioned design process and methodology. Codes of the models could be easily translated into SystemC or SystemVerilog.

Section 2 summarizes event-triggered and time-triggered communication. Section 3 proposes stepwise exploration of communication. Section 4 and 5 verifies the communication models in SpecC. Section 6 mentions some related works, and contains concluding remarks.

2 Event-Triggered and Time-Triggered Communication

There are two major categories for network communication in distributed embedded systems: event-triggered and time-triggered. Event-triggered communication is flexible, and appropriate for soft real-time systems. Time-triggered communication, on the contrary, is deterministic, in the sense that all instants of message transmission are scheduled beforehand. This is suitable for applications in which the data traffic is of a periodic nature, and this ensures dependable hard real-time message delivery which is necessary in safety-critical applications.

Both the above have two sub-categories: centralized and decentralized. In centralized event-triggered/time-triggered communication, a single arbiter/scheduler manages the whole network. In decentralized event-triggered/time-triggered communication, each module is responsible for arbitration/scheduling. The former is less expensive and easier to implement, while the latter is faster, and more robust due to the absence of a single point prone to failures and load concentration.

For example, below are some protocols for in-vehicle networks:

- CAN (Controller Area Network) [4,5,6]: a broadcast, differential serial bus standard. Its bit rates is up to 1 Mbps. It is decentralized event-triggered.
- LIN (Local Interconnect Network) [7]: also a broadcast serial network. It is designed as a small and economical substitute for CAN, and its bit rates is up to 20 kbps. It is centralized time-triggered.
- FlexRay [8]: next generation automotive network communications protocol. its bit rates is up to 20 Mbps. It is decentralized time-triggered.

3 Stepwise Exploration of Communication

In the conventional design process, we must select which communication protocol to use at the beginning. Once having selected any, we cannot switch to another, even if it is found later that another is better. A complex distributed embedded system may include several categories of communication, which should be selected depending on physical constraints, thus it is sometimes difficult or unable to select at the beginning. In addition, we cannot reuse a component or framework for other systems based on any other protocols.

Consequently, referring Model Driven Architecture (MDA) discipline [9], which is now widely accepted in Software Engineering, we investigate a design process of communication which begins from abstract specification without assuming any communication category, then explores the categories in a stepwise manner, and is followed by physical implementation synthesis. Fig. 2 shows the result in outline.

At the beginning, sender and receiver modules are connected by an abstract channel with virtual functions of sending and receiving. Then, the channel is transformed into a more concrete model, and there are two choices: an event-triggered channel or a time-triggered channel. The modules need no transformation. The event-triggered channel is accompanied with virtual arbiter and filter, while the time-triggered channel is with a virtual scheduler. Next come a centralized or decentralized model for each event-triggered and time-triggered channel. In the decentralized model, the function of arbitration, filtering, and scheduling are embedded in the sender and receiver modules.

At each model, a designer verifies its correctness, and then selects which way to go, considering advantages of each path such as presented in Section 2, based on some estimation or profiling which reflect requirements and constraints. The designer makes decision, not at once at the beginning, but in a stepwise manner gradually fixing details. Also, the designer verifies the system, not at once after implements it, but in a stepwise manner.

4 SpecC Interpretation of Communication Models

This section presents interpretation of each of the seven communication models mentioned above. The results are codes in SpecC, which can be executed and verified. Here, only essential parts of some codes are shown.

(1) Abstract Communication Model: Each pair of sender-receiver has its own virtual communication line which is simulated by a shared variable with synchronization (Fig. 3). `I_snd` and `I_rcv` are interfaces of `Chnl` which connects two behaviors `Sender` and `Receiver`. `Chnl` has an array of shared variables `line`, each of which simulates a communication like corresponding to each `Receiver` instance. ID's are assigned to the behaviors elsewhere. An array of event `e` is for synchronization between the `Sender` and `Receiver`.

(2) Event-Triggered Communication Model: The virtual and per-ID synchronization is replaced by an arbiter and a filter for event-triggered

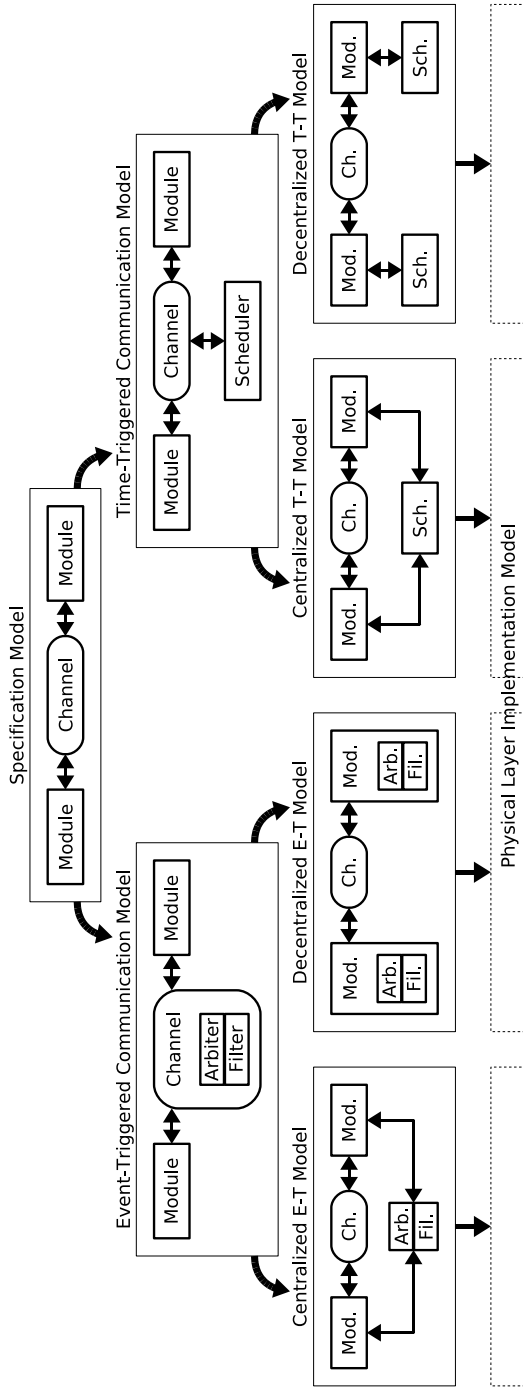


Fig. 2. Stepwise Exploration of Communication Models

```

interface I_snd {
    void send(ID i,DATA d); };
interface I_rcv {
    DATA receive(ID i); };
channel Chnl(void)
    implements I_snd,I_rcv {
    DATA line[MAX];
    event e[MAX];

    void send(ID i,DATA d) {
        line[i]=d;
        notify(e[i]); }

    DATA receive(ID i) {
        wait(e[i]);
        return line[i]; } };
behavior Sender(I_snd s) {
    ID receiver_id;
    DATA d;

    void main(void) {
        ...
        s.send(receiver_id,d); } };
behavior Receiver(I_rcv r) {
    ID my_id;
    DATA d;

    void main(void) {
        d=r.receive(my_id);
        ... } };
behavior System(void) {
    Chnl ch;
    Sender s1(ch);
    Receiver r1(ch);

    void main(void) {
        par{
            s1.main();
            r1.main(); } } };

```

Fig. 3. SpecC Code for Abstract Communication Model

communication (Fig. 4). The sender's and receiver's behaviors remain the same as in (1), and are omitted from the figure. Now, the `Chnl` contains an `Arbiter` and `Filter` so that all the communications share a single line. The variable `use` is set when any communication occupies the line.

(3) Time-Triggered Communication Model: The virtual synchronization is replaced by a scheduler for time-triggered communication (Fig. 5). The sender's and receiver's behaviors remain the same as in (1), and are omitted from the figure. Now, the `Chnl` shares with the `Scheduler` a variable `slot_id`, which indicates a scheduled time slot assigned to an ID for communication.

(4) Centralized Event-Triggered Communication Model: The arbiter and the filter are raised from the inner behavior within the channel to the top-most behavior. The structure of codes remain almost the same as in (2), and is omitted in this paper.

(5) Decentralized Event-Triggered Communication Model: The arbiter and filter are duplicated, and placed into the sender's and receiver's behaviors respectively (Fig. 6). The channel is replaced by a simple wire for transmission, and the senders and the receivers share this single wire. The receiver *senses* the wire to identify whether the communication is to itself or not.

(6) Centralized Time-Triggered Communication Model: The scheduler is coordinated with the sender and receiver, not with the channel as in (3). The structure of codes remain almost the same, and are omitted in this paper.

```

struct PACKET {DATA d, ID i};
channel Chnl(void)
  implements I_snd, I_rcv {
channel Arbiter(void)
  implements I_set, I_reset {
  int use=0;

  void set(void) {
    while (use) {
      waitfor(1); }
    use=1; }
  void reset(void) {
    use=0; } };

channel Filter(void)
  implements I_check {

  int check(ID i1, ID i2) {
    return(i1==i2); } };

  void send(ID i, DATA d) {
    arb.set();
    p.d=d;
    p.i=i; }
  DATA receive(ID i) {
    while (!fil.check(i, p.i)) {
      waitfor(1); };
    arb.reset();
    return p.d; } };

```

Fig. 4. SpecC Code for Event-Triggered Communication Model

```

behavior Scheduler(
  out ID slot_id) {
  ID table[MAX];
  int k;

  void main(void) {
    k=0; while (1) {
      slot_id=table[k];
      k++;
      if (k>=MAX) { k=0; };
      waitfor(1); } } };

channel Chnl(in ID slot_id)
  implements I_snd, I_rcv {
  DATA slot;

  void send(ID i, DATA d) {
    while (i!=slot_id) {
      waitfor(1); };
    slot=d; }
  DATA receive(ID i) {
    while (i!=slot_id) {
      waitfor(1); };
    return slot; } };

```

Fig. 5. SpecC Code for Time-Triggered Communication Model

```

behavior Sender(I_wire w) {
  ID receiver_id;
  DATA d;

  void main(void) {
    ...
    while (w.sense()) {
      waitfor(1); }
    w.transmit(receiver_id);
    w.transmit(d); } };

behavior Receiver(I_wire w) {
  ID my_id, i;
  DATA d;

  void main(void) {
    while ((i=w.sense())
      && (my_id != i)) {
      waitfor(1); };
    d=w.sense()
    ... } };

```

Fig. 6. SpecC Code for Decentralized Event-Triggered Communication Model

| | |
|--|--|
| <pre>behavior Sender(I_wire w) { Scheduler sch(slot_id); ID receiver_id; DATA d; void main(void) { par{ sch.main(); } ... while (receiver_id !=slot_id) { waitfor(1); }; w.transmit(d); } } };</pre> | <pre>behavior Receiver(I_wire w) { Scheduler sch(slot_id); ID my_id; DATA d; void main(void) { par{ sch.main(); } while (my_id !=slot_id) { waitfor(1); }; d=w.sense(); ... } } };</pre> |
|--|--|

Fig. 7. SpecC Code for Decentralized Time-Triggered Communication Model

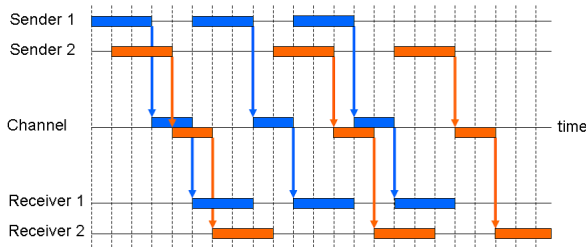
(7) **Decentralized Time-Triggered Communication Model:** The scheduler is duplicated, and moved into the sender's and receiver's behaviors (Fig. 7). The channel is replaced by a simple wire for transmission, and the senders and the receivers share this single wire. The sender's `Scheduler` instance and the receiver's `Scheduler` instance synchronizes so that they give consistent scheduling.

```
abstract model:
0000 Sender1: start
0001 Sender2: start
0003 Sender1: send
0003 Channel: Sender1 to Receiver1 start
0004 Sender2: send
0004 Channel: Sender2 to Receiver2 start
0005 Sender1: start
0005 Channel: Sender1 to Receiver1 end
0005 Receiver1: receive
0006 Channel: Sender2 to Receiver2 end
0006 Receiver2: receive
0008 Sender1: send
0008 Channel: Sender1 to Receiver1 start
0009 Sender2: start
0010 Sender1: start
0010 Channel: Sender1 to Receiver1 end
0010 Receiver1: receive
0012 Sender2: send
0012 Channel: Sender2 to Receiver2 start
0013 Sender1: send
0013 Channel: Sender1 to Receiver1 start
0014 Channel: Sender2 to Receiver2 end
0014 Receiver2: receive
```

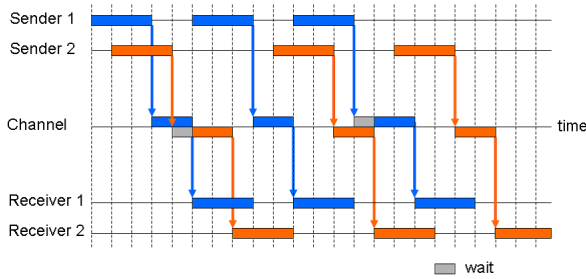
Fig. 8. Execution Log of the Abstract Model

5 Experiments

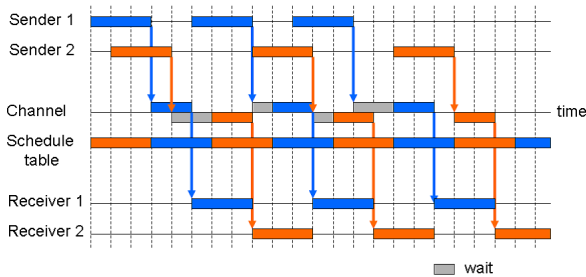
We have verified all the seven models appeared above, by implementing all the full codes. All the models must preserve the same behavior (in the general sense) as the abstract communication model that sends and receives data in an arbitrary order. The event-triggered communication model and its centralized and decentralized sub-models use a single wire which all the sender-receiver pair share by arbitration as well as preserving the behavior of the abstract communication model. The time-triggered communication model and its centralized and decentralized sub-models use a single wire, not by arbitration but by time-slicing scheduling.



(a) Abstract Model



(b) Event-Triggered Model



(c) Time-Triggered Model

Fig. 9. Execution Sequences of Design Process for Embedded Systems

Here we present some execution logs. Fig. 8 is an log extract of the abstract model. Fig 9 is a set of schematic sequence representations of logs of the abstract model, the event-triggered model, and the time-triggered model, respectively. These confirm that our models work properly.

6 Concluding Remarks

Stepwise exploration encourages stepwise decision making, component and framework reuse, and early stage verification, all of which accelerate design processes. This paper applies it to design of distributed embedded systems, as the first step to communication exploration. This paper also contributes toward integrated design of event-triggered and time-triggered communication, which are used separately at present.

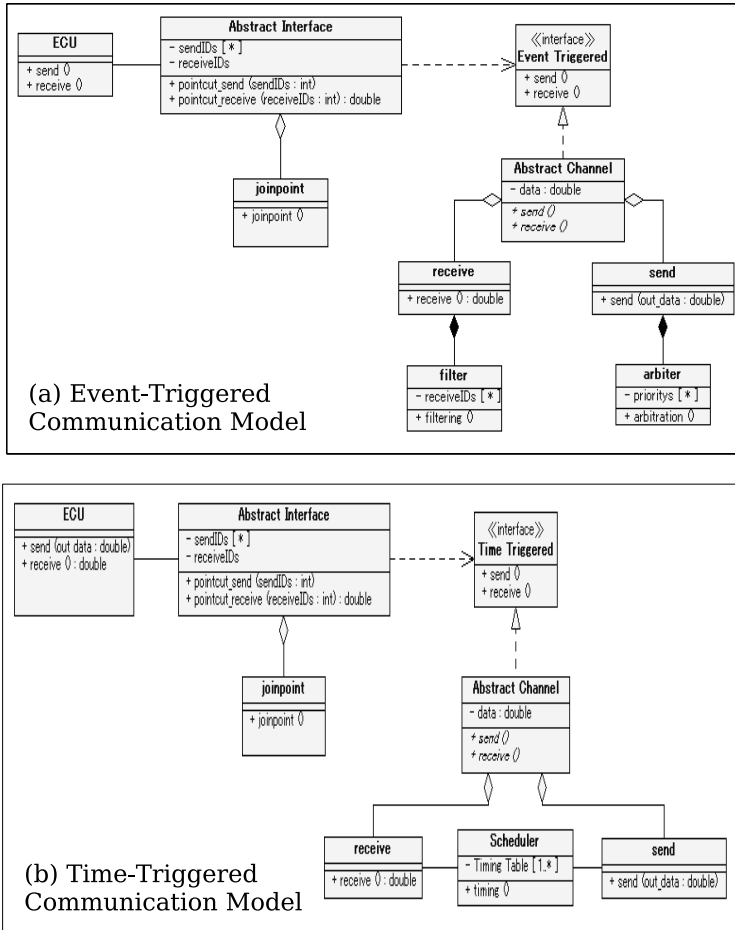


Fig. 10. UML Class Diagrams of Communication Models

There have been some researches on mixed scheduling of event-triggered and time-triggered communication [10,11], however there has been none yet on communication exploration in distributed embedded system design.

Our ongoing studies are interpreting them in Executable UML [9]. There is a research trend to apply UML and MDA to System-Level Design from a few years ago [12]. However, there has been no study on communication exploration yet.

Some models described in UML are shown in Fig. 10 as examples. The former is the class diagram for event-triggered communication model, and the latter is the one for time-triggered. “EUC” (Electronic Control Unit) is an embedded module, and “joinpoint” is a tool class for framework reuse.

We are still at the starting point of this study. Our ongoing studies are: (1) interpreting them in Executable UML as mentioned above, (2) formalizing semantics-preserving transformation between models to build an automatic CAD tool, and (3) investigating some real-world applications.

References

1. Gajski, D.D., et al.: SpecC: Specification Language and Methodology. Kluwer, Dordrecht (2000)
2. Gerstlauer, A., et al.: System Design: A Practical Guide with SpecC. Kluwer, Dordrecht (2001)
3. Kobayashi, K., et al.: Exploration of Communication Models in the Design of Distributed Embedded Systems. IEEJ Trans. on Electrical and Electronic Engineering 2(3), 402–404 (2007)
4. Robert Bosch GmbH, CAN Specification (1991)
5. ISO TC 22/SC 3, Controller Area Network (CAN), ISO 11898 (2003)
6. ISO TC 22/SC 3, Low-Speed Serial Data Communication, ISO 11519 (2005)
7. LIN Consortium, LIN Specification (1999)
8. FlexRay Consortium, FlexRay Protocol Specification (2005)
9. Mellor, S.J., et al.: MDA Distilled: Principles of Model-Driven Architecture. Addison-Wesley, Reading (2004)
10. Pop, T., et al.: Schedulability Analysis for Distributed Heterogeneous Time/Event Triggered Real-Time Systems. In: Proc. IEEE 15th Euromicro Conference on Real-Time Systems, pp. 257–266 (2003)
11. Pop, P., et al.: Schedulability-Driven Partitioning and Mapping for Multi-Cluster Real-Time Systems. In: Proc. IEEE 16th Euromicro Conference on Real-Time Systems, pp. 91–100 (2004)
12. Proc. 2006. Workshop on UML for SoC Design, in conjunction with ACM/IEEE 43th Design Automation Conf. (2006)

An End-to-End QoS Adaptation Architecture for the Integrated IntServ and DiffServ Networks

Ing-Chau Chang¹ and Shi-Feng Chen²

¹ Department of Computer Science and Information Engineering, National Changhua University of Education, Changhua, Taiwan, R.O.C.

`icchang@cc.ncue.edu.tw`

² Institute of Information Management, Chaoyang University of Technology, Wufeng, Taichung County, Taiwan, R.O.C.

Abstract. In this paper, we propose an end-to-end quality of service (QoS) adaptation network architecture to guarantee service qualities for mobile users, according to user requirements and available network resources on the end-to-end path which is across the wired backbone DiffServ network and wireless IntServ networks. Further, we adopt the bandwidth broker (BB) for resource allocations and COPS-SLS protocol for negotiating QoS in DiffServ backbone, and the context transfer protocol (CTP) on IntServ wireless networks to resolve service interruptions during handoffs. Finally, we propose a flexible and efficient bandwidth adjustment algorithm, which is based on CBQ and RED schemes, to adaptively reallocate available bandwidth among different traffic classes on border gateway routers between DiffServ and IntServ networks.

1 Introduction

It has been shown as a challenging task to provide end-to-end QoS services for users on the traditional wired network environment which is composed of access networks with the IntServ scheme [1] and the backbone network with the DiffServ [2] one [3]. Problems such as incompatibilities of these two different QoS schemes may result in breakdowns of QoS mechanisms for packets of multimedia streams in the boundary between DiffServ and IntServ domains. Researches proposed mechanisms to resolve these problems by designing an integrated framework to complement these two QoS schemes [3-4], e.g., the traffic mapping mechanism in edge routers which connect IntServ and DiffServ domains. As wide-spreading wireless networks, which adopt the IntServ QoS scheme, have become major access networks for mobile hosts (MH) in recent years, the aforementioned problems will get even worse due to the mobility of MH. Whenever the MH, who adopts the mobile IP (MIP) protocol for mobility management, hands over to a new wireless cell, the MH will suffer handoff latencies to acquire a new care-of address (CoA) and then execute binding update (BU) to its home agent (HA) before resuming the media stream through the new path. Further, the end-to-end path between the MH and the correspondent node (CN) may change, which then introduces extra operations to guarantee the end-to-end QoS on this new path. If network resources on the new path are not available, the real-time multimedia service for the MH will be interrupted, which may degrade its QoS significantly.

For guaranteeing the end-to-end QoS of the moving MH on the integrated IntServ wireless and DiffServ wired network environment, we summarize the following four necessary criteria:

1. There must be *QoS signaling protocols* between different IntServ and DiffServ network domains.
2. Because IntServ and DiffServ domains adopt totally different approaches to process user packets, there must be *traffic mapping mechanisms* between two domains to provide packets with the same QoS.
3. For reducing the handoff latency when the MH hands over to a new cell, there must be *seamless handoff mechanisms* to avoid media playback interruption.
4. There must be *QoS and service adaptation mechanisms* to dynamically adjust end-to-end service qualities of the MH to available network resources when the handoff occurs. If redundant resources are allocated to other class users, networks should re-adjust resources among all classes of MHs to satisfy the requested QoS of the high-priority MH as much as possible.

This paper is organized as follows. In section 2, we will give a survey for works on the end-to-end QoS and compare their pros and cons. In section 3, we will propose and discuss detail operations of our end-to-end QoS adaptation framework to fulfill the above four criteria. Simulation results will be shown in section 4 to exhibit efficiencies of this framework. We conclude this paper in section 5.

2 Related Works

IETF IntServ usually combines RSVP to negotiate and reserve resources on network routers by keeping the soft state information of each flow. It can achieve true per-flow QoS guarantees on small networks like LANs. However, because each IntServ router has to record the soft state information for each flow, it is not an efficient approach to deploy IntServ on WAN. Moreover, as the number of active flow changes, IntServ is not flexible enough due to the re-negotiation process of RSVP. For resolving IntServ's scalability problem, IETF proposed DiffServ for achieving per-class QoS by handling most of QoS operations on *edge routers*. As soon as user packets enter the DiffServ domain, the edge router in the domain boundary will classify these packets into different traffic classes by marking them with corresponding *DiffServ code points* (DSCP), according to the *service level agreement* (SLA) made when the user subscribes services with the network ISP. Depending on DSCP values in packet headers, the interior core router schedules these packets with different precedence values, which are called as their *per-hop-behaviors* (PHB). Consequently, DiffServ is more appropriate on wide-area backbone networks than on local-area networks.

For integrating the wired DiffServ backbone and IntServ LANs to achieve end-to-end QoS support, researches [3-4] work on the traffic mapping issue by proposing the *common open policy service* (COPS) [5] as the signaling protocol to dynamically negotiate user requirements and resource allocations with the bandwidth broker (BB) [6] on the DiffServ domain. RSVP control messages on the IntServ domain are not

processed in the DiffServ one to reduce complexities on core routers. However, without considering how to manage user mobility on wide-spreading wireless LANs which adopt the IntServ approach, these works only satisfy criteria 1 and 2.

Trossen and Chaskar [7] proposed to use Session Initial Protocol (SIP) [8] for initial session negotiation between the MH and the transmitter under heterogeneous networks. While the MH is going to change its network attachment point, the current access router (AR) of the mobile will directly transfer the user information to the new AR. With this kind of *application context transfer*, this approach reduces the original SIP latency for re-negotiation. Consequently, it satisfies criteria 1 and 3. However, this work has not mentioned how to handle the inconsistent situation when the new AR cannot support the same amount of resources as the current one does, which fails to meet criterion 4. Further, the authors omitted mechanisms of how to map traffics on different domains with their SIP-based approach, which violates criterion 2.

The network architecture proposed by Chaouchi and Pujolle [9] also consists of a DiffServ backbone network and IntServ wireless LANs. If MHs want to enable new services or change service requirements, they will adapt *MCOPS* (Mobile COPS) as a signaling protocol, which meets criterion 1. As for criterion 2, they defined a direct traffic class mapping between the WLAN and the DiffServ. Major contributions of this paper are *Anticipated Handoff* and *Adaptive Handoff* for criteria 3 and 4, respectively. The anticipated handoff uses user requirements recorded in the policy base of the server to predict possible moving directions and work on the handoff proactively when the mobile entered the overlapped area of two wireless cells. Depending on resources of the mobile's new location, the adaptive handoff adjusted QoS of the MH at the new location or reserved resources for the user in advance.

3 System Architecture

Characteristics of our proposed architecture, shown in Fig. 1, are listed as follows:

- (1) The wired backbone is based on IETF RFC 2998 DiffServ architecture and each DiffServ domain is equipped with a *bandwidth broker* (BB) [6] to manage internal resources and search for the optimal route in the domain.
- (2) Local wireless networks are configured to support IntServ. We use *RSVP* as an end-to-end signaling protocol because RSVP is a receiver-oriented one, which is appropriate to handle the change of resource requirements after the MH's handoff.
- (3) For supporting uninterrupted services after the MH's handoff, we integrate the *Context Transfer Protocol* (CTP) [10], which was proposed by SEAMOBLY [11], to transfer the MH's current context from the old access router (AR) to the new one for accelerating the handoff process as soon as CTP receives the layer 2 handoff trigger. Further, we modify the original context by adding new QoS parameters such that the new AR is able to optimally allocate its network resources to meet requirements of this moving mobile for continuing its services. In this way, our architecture fulfills criterion 3.
- (4) We adapt *COPS-SLS* [12], which inherits concepts of COPS, as a negotiation protocol to dynamically adjust resources between wired and wireless networks. With it, criterion 1 can be achieved.

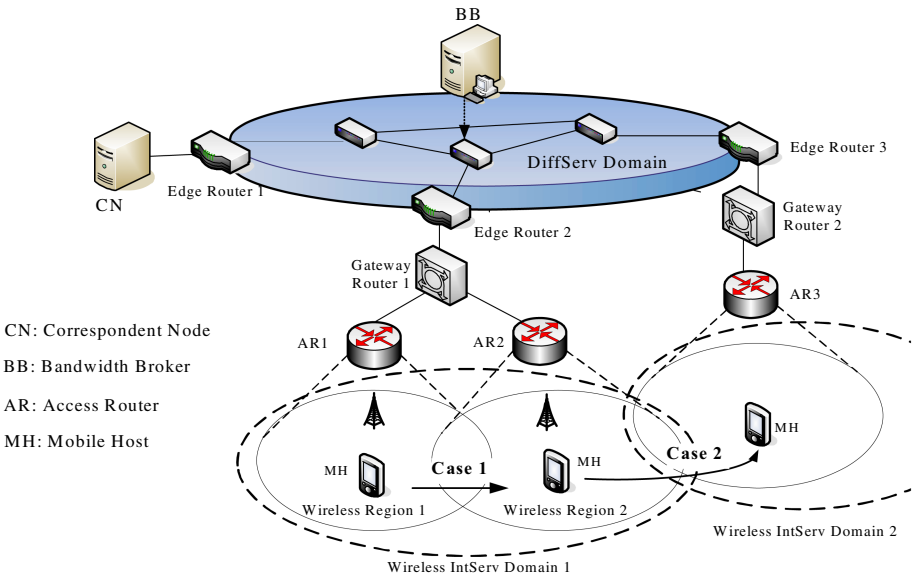


Fig. 1. The proposed end-to-end QoS adaptation architecture

3.1 Proposed Handoff Flow

In this proposed architecture, the following procedures shown at the first stage for RSVP initialization in Fig. 2 must be executed to start a service:

- a. When the MH wants to start its service, the CN will use RSVP to issue a PATH message at step 1.1 in Fig. 2, which contains TSPEC, PHOP (Previous Hop Router Address) [13] and ADSPEC for QoS, to the MH. This PATH message is considered as a normal traffic one when it passes through the DiffServ domain.
- b. After the MH receives the RSVP PATH message from the CN, it will send back an RSVP RESV message along the reverse path of PATH. While this message arrives at the edge router, i.e., ER2, of the DiffServ domain, it will retrieve QoS requirements from this message and convey them to the BB by COPS-SLS at step 1.2. The BB will record these QoS requirements and corresponding policy configurations. After that, the edge router will forward the RESV message back to the CN to complete the end-to-end signaling process at step 1.3.
- c. CN begins its transmission to the MH at step 1.4.

In the following, we will describe how to achieve the end-to-end QoS adaptation in our proposed architecture for the *Intra-IntServ-domain handoff* and *Inter-IntServ-domain handoff*.

Case 1. As shown in Fig. 2, when the MH moves from the service range of AR1 to AR2 under the same Gateway Router1, this kind of handoff is called *Intra-IntServ-domain handoff* with the following five processing stages.

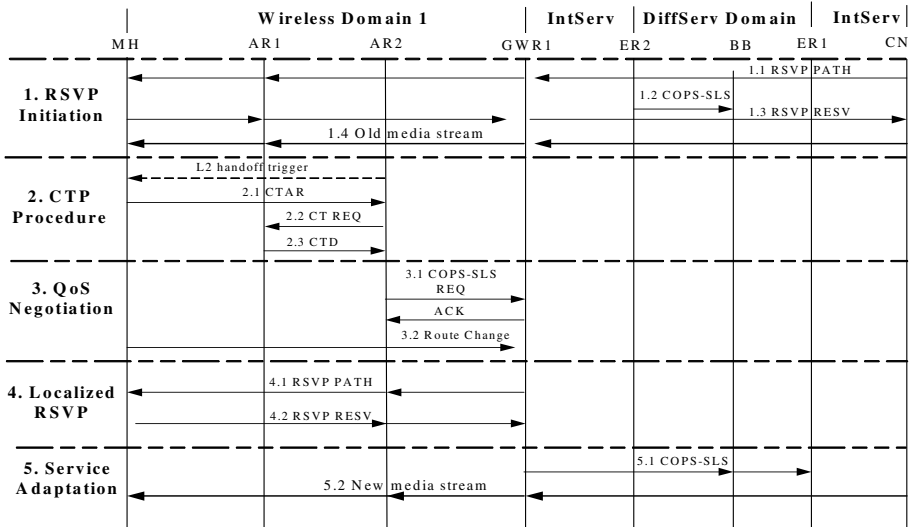


Fig. 2. Flow of the Intra-IntServ-domain handoff

(1) RSVP initialization

As mentioned above, RSVP procedures must be executed to start a service.

(2) Handoff Start and CTP Procedure

- a. When the MH enters the overlapped range between the wireless region 1 and 2 under the wireless IntServ domain 1, it recognizes it is going to perform the Intra-IntServ-domain handoff process within the IntServ domain 1.
- b. While the MH receives the beacon signal, i.e., Layer 2 handoff trigger, of AR2 in the wireless region 2, the CTP process starts. As shown in Fig. 2, the MH will issue a *Context Activate Request* (CTAR) to AR2 at step 2.1 and then AR2 will send a *Context Request* (CT Request) to the original AR1 in the wireless region 1 at step 2.2. At last, AR1 will forward the MH’s context in the modified CTD message back to AR2 at step 2.3. The modified CTD message is shown in Table 1, including RSVP QoS parameters like the *Service Class*, *RSPEC* and *TSPEC*.

Table 1. Modified CTD format

| | | | | |
|---|----------------|-----------|--------------|---------------|
| Message Type | C | R | Rsv | Length |
| Elapsed Time (in milliseconds) | | | | |
| Mobile Node’s Previous Care-of Address | | | | |
| Mobile Node’s New Care-of Address, if C=1 | | | | |
| Type = Auth | Type Length | Algorithm | | Key Length |
| Service Class | RSPEC | | TSPEC | |

(3) QoS Negotiation and Handoff Completion

As AR2 receives the MH's context, it will try to provide enough resources to the MH. If AR2 cannot fulfill MH's resource requirements, it will degrade QoS of the MH and notify Gateway Router 1 of the degraded QoS and the changed route to the destination by COPS-SLS for continuing services of the MH at AR2, which is shown at step 3.1. Oppositely, the MH at AR2 still owns the original QoS as at AR1 if AR2 has enough network resources. Because AR2 and Gateway Router 1 do not reserve resources for the MH in advance, the MH has to issue a *Route Change* message to Gateway Router 1 via AR2 for recording the current location of the MH to be in the wireless region 2, as shown at step 3.2.

(4) Localized RSVP Procedure

- a. As Gateway Router 1 receives the Route Change message from the MH, it has recognized that the MH has moving to the new wireless region 2.
- b. For reconstructing the local path and reserving resources in the new wireless region, Gateway Router 1 will convey a new RSVP PATH message to the MH under AR2 at step 4.1 and the MH will return the RESV message back to Gateway Router 1 after accepting the PATH message at step 4.2.

(5) Service Adaptation

If the localized RSVP procedure changes network resources allocated to this MH, GWR1 will adopt COPS-SLS to transmit modified QoS requirements to BB in the DiffServ backbone domain. Then BB will update configurations in the MH's policy database and issue modified policies to ER1 by COPS-SLS. Then, ER1 will adjust priorities, i.e., DSCP values, of MH packets entered into the DiffServ domain according to these modified policies at step 5.1. Finally, the media stream will follow the new path to the MH via GWR1 and AR2 as shown at step 5.2. In this way, our architecture fulfills criterion 4.

Case 2. When the MH moves from the service range of AR2 under Gateway Router 1 of the IntServ domain 1 to AR3 under Gateway Router 2 of the IntServ domain 2, which is called *Inter-IntServ-domain handoff*, our architecture will perform the following five processing stages as shown in Fig. 3.

(1) RSVP initialization

As mentioned above, RSVP procedures must be executed to start a service.

(2) Handoff Start and CTP Procedure

This stage is similar to stage 2 of the Intra-IntServ-domain handoff, except operations are executed between the original AR2 in IntServ domain 1 and the new AR3 in the IntServ domain 2 as shown in Fig. 3. Steps to send CTAR, CT Request and CTD messages are numbered as step 2.1, 2.2 and 2.3 respectively.

(3) QoS Re-negotiation and Handoff Completion

- a. As AR3 receives the MH's context and it cannot fulfill MH's resource requirements, it will degrade the MH's QoS and notify Gateway Router 2 in the new IntServ domain of the degraded QoS by COPS-SLS for continuing services of the MH at AR3, which is shown at step 3.1 in Fig. 3.
- b. Gateway Router 2 will allocate the most appropriate resources after negotiation between the MH's requirements and its current available resources. Then it will adopt COPS-SLS to transmit negotiated QoS parameters to the BB in the Diff-Serv domain, as shown at step 3.2 in Fig. 3.

- c. Oppositely, if AR3 can fulfill resource requirements of the MH, the MH has to issue a *Route Change* message to Gateway Router 2 via AR3 in the IntServ domain 2 as shown at step 3.3.
 - d. As Gateway Router 2 receives the Route Change message from AR3, it will recognize the MH is performing an Inter-IntServ-domain handoff such that it will further issue a Route Change message to the CN for re-executing the end-to-end RSVP signaling at step 3.3.
- (4) Re-routing and Re-configuration
- a. Whenever the BB in the DiffServ domain receives negotiated QoS parameters from Gateway Router 3, it adopts SNMP/OSPF to re-configure resources among interior routers and find a new optimal route for the MH to satisfy its QoS, i.e., QoS routing, in the DiffServ domain, which is shown at step 4.1.
 - b. Then BB will update the MH's policy database and issue modified policies to ER1 by COPS-SLS. Finally, ER1 will adjust DSCP values of MH packets entered into the DiffServ domain as shown at step 4.2.
- (5) End-to-End RSVP Signaling
- a. As soon as the CN receives the Route Change message from Gateway Router 2 and recognizes the MH has moving to a new IntServ domain, it has to release old resources and re-execute the new end-to-end RSVP signaling process.
 - b. The CN will issue a new PATH through Gateway Router 2 and AR3 to the MH and the MH will return an RESV back to the CN as shown at steps 5.1 and 5.2 respectively. In this way, this architecture provides the media stream an end-to-end QoS adaptation in the integrated networks as shown at step 5.3.

3.2 Traffic Mapping Mechanism

In the integrated IntServ and DiffServ networks, traffics of user services will pass through IntServ for the wireless LAN and DiffServ for the wired backbone. In IntServ, three different traffic types are defined as the *guaranteed service* (GS), *control load service* (CLS) and *best effort* (BE). DiffServ also provides *expedited forwarding* (EF), *assure forwarding* (AF) and *best effort* (BE) services for classifying user packets and determining priorities of them, according to the multi-fields classifier which consist of characteristics of these packets or payment policies chosen by users.

For reducing the processing overhead to convert the traffic type from the IntServ domain to the DiffServ domain, and vice versa, at the edge router, our architecture follows the traditional concept to provide an one-to-one traffic mapping in Table 2 between these two domains. Because both the GS traffic in IntServ and the EF one in DiffServ aim to provide the steady and seamless service, we map these two traffics directly. For the CLS traffic in IntServ, we further propose three sub-classes, i.e., CLS Real-time (CLS_{RT}), CLS Multimedia (CLS_{MM}) and CLS Control Message (CLS_{CM}), and map them into three different AF classes, i.e., AF1 to AF3, with different queue management priorities in DiffServ. According to the work done by AQUILA [14], we also define corresponding rules for traffic parameters and algorithms for our traffic mapping. In this way, our architecture fulfills criterion 2.

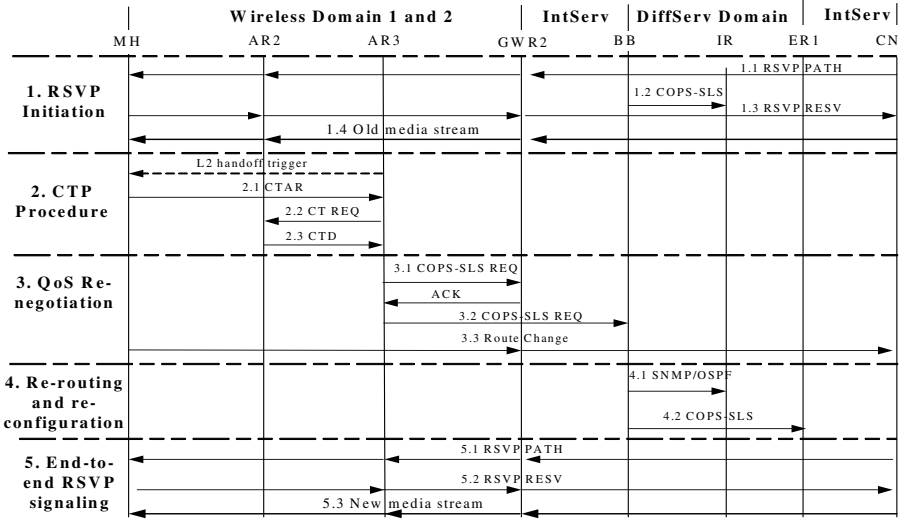


Fig. 3. Flow of the Inter-IntServ-domain handoff

Table 2. Traffic mapping table in our approach

| Traffic Class | | Service Descriptions |
|-------------------|-------------------|----------------------|
| IntServ | DiffServ | IntServ/DiffServ |
| GS | EF | Virtual Leased Line |
| CLS _{RT} | AF ₁₋₃ | Real-time Traffic |
| CLS _{MM} | | Multimedia Data |
| CLS _{CM} | | Control Message |
| BE | BE | General Packet |

3.3 QoS and Service Adaptation

For providing dynamic QoS and service adaptation, we adopt the *class-based queuing* (CBQ) [15] and *random early detection* (RED) [16] to manage traffic queues in the gateway router which manages underlying wireless LANs. In CBQ, a single queue is facilitated for each traffic class, which may contain multiple user connections with similar characteristics. Each class can borrow its available network bandwidth to another class if allowed in its initial configuration. On the other hand, RED provides the queue management mechanism for forthcoming congestion. It will first mark or drop packets when they arrive at the queue and may notify the traffic source to reduce the emission rate for mitigating the congestion. By integrating the multi-queue management of RED and bandwidth sharing of CBQ, we propose an adaptation algorithm, which is denoted as CBQ+RED in this paper, in the IntServ gateway router to handle the situation when the associated queue of the user traffic does not have enough bandwidth to meet the user’s requirement. This algorithm is shown in Table 3.

Table 3. The proposed CBQ+RED QoS adaptation algorithm

| |
|---|
| <p>For each GS packet arrival Calculate average queue size $avg(GS)$ If $[\min_th(GS) \leq avg(GS) < Max_th(GS)]$ Calculate packet drop probability $P\alpha$ $P\alpha = P_{Max} \times [(avg(GS) - \min_th(GS)) / ((Max_th(GS) - \min_th(GS))]$ Mark the arriving GS packet with probability $P\alpha$ Else if $[MAX_th(GS) \leq avg(GS)]$ then Calculate the congestion level V of the GS class $V = \frac{[(avg(GS) + \sum_{i=1}^n incoming_pkt(i)) - Max_th(GS)]}{[(GS\ queue\ length) - Max_th(GS)]}$ Calculate average queue size of CLS_{RT} and CLS_{MM}, i.e., $avg(CLS_{RT})$ and $avg(CLS_{MM})$ If $[\min_th(CLS_{RT, MM}) \leq avg(CLS_{RT, MM}) < Max_th(CLS_{RT, MM})]$ // $(CLS_{RT}$ and/or $CLS_{MM})$ have redundant bandwidths to lend to GS GS borrows BBW bandwidth from CLS_{RT} and CLS_{MM}, where $BBW = V \times \{ [Max_th(CLS_{RT}) - avg(CLS_{RT})] + [Max_th(CLS_{MM}) - avg(CLS_{MM})] \}$ If $\{BBW \leq [avg(GS) - Max_th(GS)]\}$ // if BBW is not enough for all incoming GS packets Re-mark remaining GS packets as $CLS_{RT, MM}$ packets Re-calculate drop probabilities $P\alpha$ of $CLS_{RT, MM}$ With probabilities $P\alpha$, mark $CLS_{RT, MM}$ packets Else if $[Max_th(CLS_{RT, MM}) \leq avg(CLS_{RT, MM})]$ // CLS_{RT} and/or CLS_{MM} have no redundant bandwidths Drop the incoming GS packet</p> |
|---|

In the following, we will take the GS traffic as an example to explain how this algorithm works. Packets of the GS traffic have the highest priority among all traffic classes in IntServ. As the sum of the average queue length $Avg(GS)$ and the incoming packet length of GS traffic is approaching to its maximal threshold $Max_th(GS)$ in RED, the dropping probability of the incoming packet is raised accordingly. At last, any incoming GS packet will be dropped when the GS queue length is equal to $Max_th(GS)$. Hence, we modify the CBQ bandwidth sharing mechanism to solve the dropping problem of GS packets by borrowing sparse bandwidth from lower-priority CLS classes. The amount of borrowed bandwidth is determined by the congestion value (V) of the GS queue in Equation 1. The larger value of V means the congestion in the GS queue is more severe because the sum of the average GS queue length and incoming GS packet lengths is larger than $Max_th(GS)$ such that incoming packets have higher probabilities to be dropped. If it happens, our algorithm will first try to borrow redundant bandwidths from classes with lower priorities.

$$V = \frac{[(avg(GS) + \sum_{i=1}^n incoming_pkt(i)) - Max_th(GS)]}{[(GS\ queue\ length) - Max_th(GS)]} \quad (1)$$

Where n is the number of incoming GS packets in the past.

This algorithm has to consider the following two issues:

- (1) Which class with the next lower priority has redundant bandwidth to lend?
- (2) What amounts of bandwidth can be borrowed from this class?

Because arrival times and amounts of incoming packets are depending on specific traffic characteristics of active services, our algorithm uses the congestion level of GS class queue, i.e., the value of V , to calculate the borrowed bandwidth (BBW) from CLS_{RT} and CLS_{MM} , as formulated in Equation 2.

$$BBW = V \times \{[Max_th(CLS_{RT}) - avg(CLS_{RT})] + [Max_th(CLS_{MM}) - avg(CLS_{MM})]\} \quad (2)$$

If the next priority CLS classes do not have enough redundant bandwidth to lend to GS, our algorithm will then degrade remaining high-priority GS packets to be low-priority CLS ones by re-marking them to continue their services, instead of dropping them immediately in traditional RED. However, if CLS classes are also congested, our algorithm is obligated to drop the incoming GS packets.

4 Simulation

As mentioned above, our proposed architecture provides the gateway router in the wireless region with the integrated CBQ+RED QoS adaptation algorithm to dynamically adjust user traffics to an appropriate class queue for the best QoS guarantee and wireless bandwidth utilization. In this section, we will execute simulations to exhibit results of this proposed algorithm.

4.1 Simulation Environment

With the MATLAB v7.01 and its embedded Simulink for designing the module of our class queues, we conduct this simulation in the gateway router of the IntServ domain with five queues for the GS, CLS_{RT} , CLS_{MM} , CLS_{CM} and BE traffic classes. We assume the bandwidth of each wireless region is 11Mbps, which is further divided into five parts for these five CBQ class queues, as listed in Table 4. The Max_th value of each class queue is 90% of its allocated bandwidth. Moreover, different class queues are assumed to handle packets with different packet length distributions. GS packet lengths are ranged from 32Kb to 256Kb with the average value of 190Kb; CLS_{RT} and CLS_{MM} packet lengths are ranged from 32Kb to 256Kb with the average value of 136Kb. The CLS_{CM} class is assumed to have the shortest packet lengths of 32Kb, which means most small-size control messages can reach its destination without suffering congestion and packet dropping at the gateway router.

Table 4. Bandwidth allocations for five class queues at the gateway router

| Queue Class | GS | CLS_{RT} | CLS_{MM} | CLS_{CM} | BE |
|-----------------|-------|------------|------------|------------|-------|
| Proportion | 30% | 25% | 20% | 15% | 10% |
| Queue size (KB) | 3,300 | 2,750 | 2,200 | 1,650 | 1,000 |

4.2 Simulation Results

Simulation results for consumed bandwidths of GS and CLS_{RT} over simulation times without using the integrated CBQ+RED QoS adaptation algorithm in the gateway router are shown in Fig. 4. As described above, Max_{th}(GS) and Max_{th}(CLS_{RT}) are set as 90% of GS and CLS_{RT} allocated bandwidths, which are 2970Kbps and 2475Kbps and illustrated as two horizontal dotted lines in Fig. 4. As shown at 40 second in Fig. 4, the GS queue length is close to its Max_{th} limit of 2970Kbps and this class is considered as congested. Most incoming large-size GS packets will be dropped to keep the GS queue length below its Max_{th} limit. However, because the CLS_{RT} queue length is below 1500Kb, which is much less than its Max_{th} limit of 2475Kbps at the same time, it means the CLS_{RT} class has low bandwidth utilization and owns redundant bandwidth that can lend to the GS class.

Fig. 5 shows simulation results by applying our CBQ+RED scheme on GS and CLS_{RT} packets at the gateway router. The congestion of GS traffic occurs at 40 second in Fig. 4 does not happen again with CBQ+RED. It is because the Max_{th} limit of the GS traffic is raised from 2970Kb to 3425Kb by borrowing 70%, i.e., the current value of V, of redundant bandwidth, i.e., $(2475\text{Kb} - 1824\text{Kb} = 651) \times 70\% = 455\text{Kb}$, from the CLS_{RT} traffic. In this way, the GS queue continuously accepts incoming GS packets such that its queue length is increased until the new Max_{th} limit of the GS traffic is reached at 57 second. Oppositely, though the Max_{th} limit of the CLS_{RT} traffic is decreased from 2475Kb to 2020Kb after lending its 455Kb to the GS traffic, the CLS_{RT} class still performs well without suffering congestion. As listed in Table 5, our CBQ+RED scheme at 57 second can increase the total bandwidth utilization by 6% as compared to the traditional scheme without CBQ+RED.

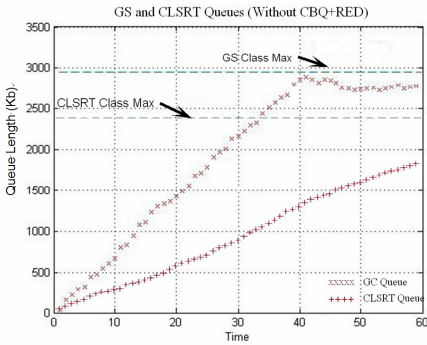


Fig. 4. Queue lengths of the GS and CLS_{RT} classes without CBQ+RED

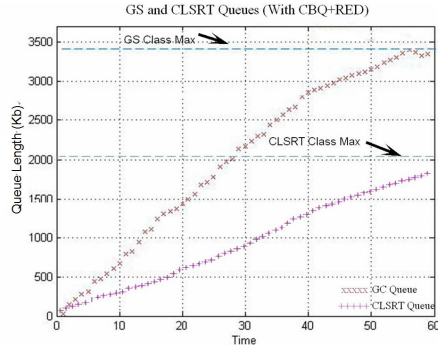


Fig. 5. Queue lengths of the GS and CLS_{RT} classes with CBQ+RED

Table 5. Bandwidth utilization at 57 second with or without the CBQ+RED scheme

| Without CBQ+RED | With CBQ+RED |
|--|--------------------------------|
| Bandwidth Utilization $(2,765+1,745)/11,000 = 41 \%$ | $(3,425+1,745)/11,000 = 47 \%$ |

5 Conclusions

In this paper, we propose an end-to-end QoS adaptation architecture with four capabilities: 1. the CTP for fast handoff; 2. the COPS-SLS as the coordination protocol between IntServ and DiffServ; 3. the CBQ+RED scheme to provide better service for the higher-priority traffic class; 4. the receiver-oriented RSVP as the end-to-end signaling protocol to continue service after the user hands over to a new wireless region. This architecture can guarantee the QoS of the higher-priority traffic class and increase total bandwidth utilization for the integrated networks.

References

1. Braden, R., Clark, D., Shenker, S.: Integrated Services in the Internet Architecture: an Overview. IETF RFC 1633 (1994)
2. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: An Architecture for Differentiated Services. IETF RFC 2475 (1998)
3. Bernet, Y., Ford, P., Yavatkar, R., Baker, F., Zhang, L., Speer, M., Braden, R., Davie, B., Wroclawski, J., Felstaine, E.: A Framework for Integrated Services Operation over Diff-serv Networks. IETF RFC 2998 (2000)
4. Bernet, Y.: The Complementary Roles of RSVP and Differentiated Services in the Full-Service QoS Network. *IEEE Communications Magazine* 38(2), 154–162 (2000)
5. Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R., Sastry, A.: The COPS (Common Open Policy Service) Protocol. IETF RFC 2748 (2000)
6. Nichols, K., Zhang, L.: A Two-bit Differentiated Services Architecture for the Internet. RFC 2638 (1999)
7. Trossen, D., Chaskar, H.: Seamless Mobile Applications across Heterogeneous Internet Access. In: *IEEE International Conference on Communications*, pp. 908–912 (2003)
8. Handley, M., Schulzrinne, H., Rosenberg, J.: SIP: Session Initiation Protocol. IETF RFC 2543 (1999)
9. Chaouchi, H., Pujolle, G.: A New Handover in the Current and Future Wireless Networks. *IEICE TRANS. Communication* E87-B(9) (2004)
10. Loughney, J., Nakhjiri, M., Perkins, C., Koodli, R.: Context Transfer Protocol (2003), <https://www1.ietf.org/internet-drafts/draft-ietf-seamoby-ctp-03.txt>
11. Seamoby Group, <http://www.ietf.org/html.charters/seamoby-charter.html>
12. Liu, C., Liu, Y., Qian, D., Li, M.: An Approach of End-to-End DiffServ/MPLS QoS Context Transfer in HMIPv6 Networks. In: *IEEE Eighth International Symposium on Autonomous Decentralized Systems*, pp. 245–254 (2007)
13. Moon, B., Aghvami, H.: Reliable RSVP PATH Reservation for Multimedia Communications under an IP Micromobility Scenario. *IEEE Wireless Communications* 9(5), 93–99 (2002)
14. AQUILA, <http://www.ist-aquila.org/>
15. Zheng, Q.: A Differentiated Service Supported Bandwidth Allocation Algorithm for Multiple Points Communications. In: *IEEE 10th International Conference on Computer Supported Cooperative Work in Design*, pp. 1–8 (2006)
16. Chen, W., Li, Y., Yang, S.H.: An Average Queue Weight Parameterization in a Network Supporting TCP Flows with RED. In: *2007 IEEE International Conference on Networking, Sensing and Control*, pp. 590–595 (2007)

Ubiquitous Laboratory: A Research Support Environment for Ubiquitous Learning Based on Sensor Networks

Mianxiong Dong¹, Kaoru Ota², Minyi Guo^{1,3}, and Zixue Cheng¹

¹ School of Computer Science and Engineering, The University of Aizu, Aizu-Wakamatsu, Fukushima 965-8580, Japan

² Department of Computer Science, Oklahoma State University, Stillwater, OK, 74077, USA

³ Department of Computer Science and Engineering, Shanghai Jiao Tong University Shanghai, 200030, China

{m5101217, minyi, z-cheng}@u-aizu.ac.jp, kaoru.ota@okstate.edu

Abstract. With the great progress of technologies, computers are embedded into everywhere to make our daily life convenient, efficient and comfortable. In the learning field, ubiquitous technologies make it possible to provide services to learners anytime and anywhere in the real world. In this paper, we present an ubiquitous environment to support college students, professors, and visitors in a laboratory to encourage positive research activities. Actions of people in the Ubiquitous Laboratory (U-Lab) are individually detected by sensor networks and analyzed to provide supports. Based on these collected information, U-Lab provides services such as to grasp a precise research progress and share research information among students and professors. We also propose a method to advise students to improve their research activities. As a case study, we implemented a Ubiquitous Corner (U-Corner) to prove our proposal is useful and practical.

Keywords: Ubiquitous Computing, Context Aware, Sensor Network, RFID.

1 Introduction

In recent years, many researchers have extensively studied on WBT (Web-Based Training) and E-learning to collect learner's study histories and give him/her study advice [3] [4] by using the internet. Some universities have already offered e-learning programs for students [1] [2]. However, in the real world a learner's study time is abundant, and study support which based on individual situation is insufficient by only using WBT and E-learning. Therefore, ubiquitous technology is applied to the learning field to meet this challenge. In a ubiquitous learning environment, service required for a user can be provided without demanding intentionally. Moreover, it comes to be able to provide the study support more individually through context information (e.g. location, time, actions, etc) corresponding to individual data which can be acquired in the ubiquitous environment. So far, many context-aware applications are developed by some research laboratories or some universities [5]. Some are used in offices to manage

employee's entering leaving information or to assist conference attendants. The others are systems for tourist guiding assisting. Almost all of them are for enterprises.

In this research, we mainly focused on the educational field. Laboratory is a central place for college students to study and research. Students usually spend a lot of time in the laboratory to do their research activities such as doing exercises, writing papers, making presentations, and implementing systems. However, because the life styles and schedules of students are different, it is not easy to share information and have communications among students and teachers. Furthermore, following the trend of the current times, there is a demand to open laboratory for a regional contribution, university-business innovation and international exchange. To answer these demands, Ubiquitous Laboratory (U-Lab) is presented in this paper. Then we propose a method to analyze the similarity and the difference between objects and/or persons based on data from sensor networks by using Euclidean Distance. This method is the base of several services in U-Lab. For example, the system should grasp a similarity between books and a student's interest when the student borrow some books from a book shelf in the laboratory. If the similarity becomes clear, the system can give certain advice which book is the best for the student. We also implemented a ubiquitous environment; U-Corner, as a test case of the Ubiquitous Laboratory. Through this implementation, we stepped out as a first step of the whole design of U-Lab. U-Corner is a partial space of the laboratory. It is filled with a lot of special tile. These tiles can collect the activity data of people based on a sensor network. By using these data, we can get semantic information subsequently and give people who are visiting U-Corner useful support.

Some works have been done on support methods in the ubiquitous learning field, such as a proposal of a personalized ubiquitous education support environment [6]. This research gives priority to lower class students, like elementary school students rather than college students. And it is mainly aiming at managing learner's lifestyle and study custom. The other research has proposed to utilize mobile and ubiquitous computing technology such as access points, iPAQs, tablet PCs, and RFIDs in the field [12]. It aims to support and improve academic activities in an original model of learning environment and especially focuses on learning in the field of Computer Engineering. In [11], not only for schools, but also for kindergartens' learning support method has been proposed. With the progress of researches of ubiquitous computing, network hardware and infrastructure have been going to be completed. The field of sensor networks is one of the most important and necessary parts for ubiquitous computing. Three kind of wireless sensor nodes such as wearable, portable, or embeddable nodes have been developed from the viewpoint of hardware [13]. By embedding computers, several sensors, RFID tags, cameras, and so on in almost all objects around elderly users in home, the users can be supported kindly and received services friendly [7]. With the high cost to realize the proposed environment, it mainly focuses on supporting older persons in daily life and constructs the whole electric house to realize it. Our research aims to utilize our existing laboratory as long as minimizing introducing the additional investments.

The remainder of this paper is structured as follows: In Section 2, our basic idea is presented. After giving the details of our method in Section 3, implementation of our system is described in section 4. We present our result and experiment in section 5. Finally, we have conclusion and discussion in Section 6.

2 Basic Ideas and the Outline of the System

The model of U-Lab is shown in Fig 1. We assumed everywhere in U-Lab is the detectable area of research, study, and the other activities. The laboratory is embedded a number of infrared sensors, RFID readers, and so forth. These devices cooperate with each other and compose one sensor network. By using this sensor network, actions of every people in the laboratory are grasped and recorded into database server. Moreover, a research progress which each student is currently doing, for example, presentation documents for a seminar, a submission status of a thesis draft, and so on, is collected by the system. The system systematically analyzes data of activities and progress state caught during a period and guess a student's life style, research effect and efficiency. Based on the results, the student receives proper supports according to one's own status by the system. Then, the system shows the results of analysis as reference to let professors know the progress of the student's research. And also, for visitors, the system provides services such as introducing the laboratory and the presenting the research achievements based on visitors' interests and visitors' level of knowledge by fully using the sensor network.

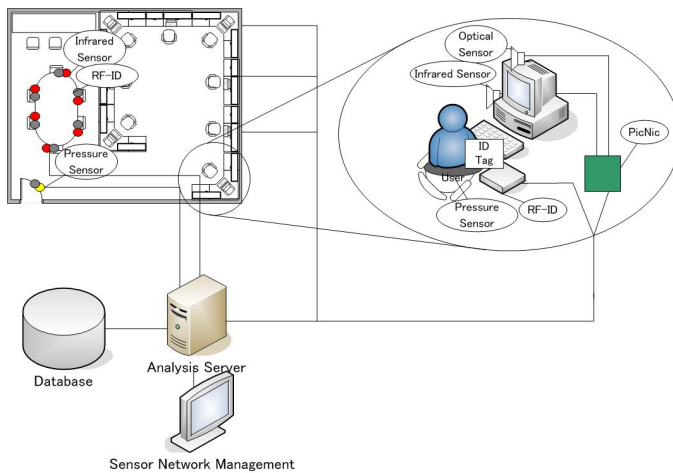


Fig. 1. The Model of the U-Lab

- How to set areas

As you can see in Fig, 2, the laboratory is divided by two areas according to detectable ranges and features of each sensor. The one area, say area A, detects whether or not a user is present in area A. If the user is present in area A, the system assumes the user does a specified activity which is assigned area A. For example, a seminar must be held if the user is in a seminar room, and the user must be reading books or some documents if the user in a room having a book shelf. The system does not consider unexpected actions such as taking a nap in a seminar room and chatting in a room having a book shelf. Like this, area A includes common spaces such as a seminar room, a room having a book shelf, and an experiment room. The other area, say area B, is a

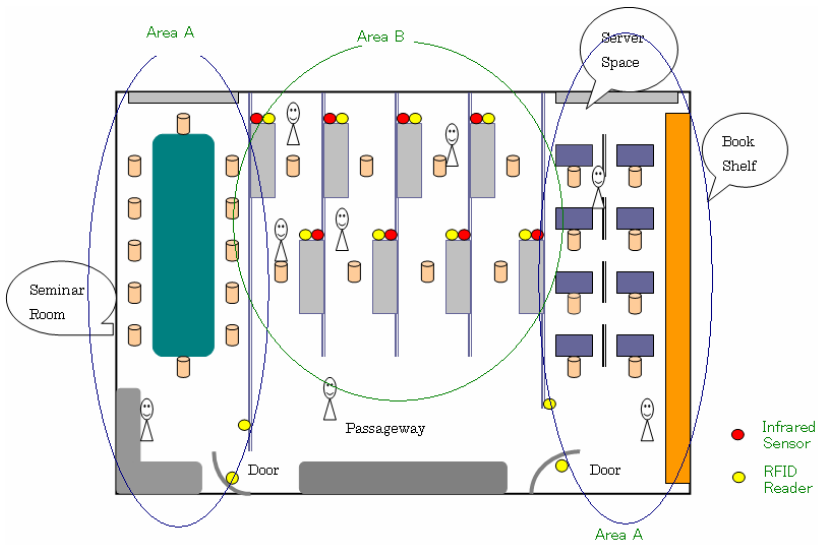


Fig. 2. An Example of Areas and Sensors Layout in U-Lab

space where a user works individually. Area B includes a personal space such as a research room having the user's desk and one's computer. Every user has one's own computer in one's own space, and we assume that every user spends almost all time in one's own space. Therefore, to analyze data of activities of each user, the system should collect not only location information, but also activity information.

- How to set sensors

To grasp a user's location approximately, the RFID readers and tags are used. RFID readers are set in both area A and area B (see Fig. 2). We assume that every user has an RFID tag every time they are in a laboratory. However, because the receivable range of RFID readers is limited, RFID readers are set at boundaries (i.e. doors) of each spaces included in area A. On the other hand, for area B, RFID readers are set in each desk because information is collected mainly from desks.

To collect activity information of each user more and more appropriately, the system uses infrared sensors which only need a few meters to detect objects and can recognize whether or not a user is present. Infrared sensors are set in each user's desk and wall of each user's space (see Fig. 2), and the system collects data of users' activities within a few meters around desks.

- How to share information among sensors

Data collected by every sensor is managed by a server. When a user passes around a detectable range of RFID readers set in boundaries (doors) of each area, readers send the server the location where the user is entering/leaving and the time when the user is entering/leaving. When an infrared sensor detects a user's actions, this data is related to information grasped by an RFID reader nearby this infrared sensor. In this case, the system assumes that the user detected by the infrared sensor and a user sensed by an RFID reader are one and the same. The server saves received data into a database and uses it for users' behavior analysis.

- How to analyze efficiently

If the system keeps collecting, saving, and analyzing users' information for a long period, each user's life style will become clear. Including time when a user comes to or leaves from a laboratory everyday, attendance rate of seminars, and behavior patterns in the laboratory, the system periodically accesses log files of a server, checks each user's status like submission of thesis drafts and submission of presentation documents, and reasons research effect and efficiency of each user. Specifically, each user's history of activities can be got by storing data of location and time detected by RFID readers to a database. As we mentioned before, when a user is in area A, the system reasons that the user is working, studying, or reading books in a common space. When a user is in area B, the system reasons that the user is studying currently only if an RFID reader set in the user's desk senses an RFID tag of the user and also an infrared sensor detects the user's action. And, visitors have particular RFID tags so that the system can distinguish them from laboratory members.

- How to support effectively

At first, each student makes one's own learning schedule with a professor's consent. It includes a seminars' schedule, time of group activities, a research schedule, time of thesis submission, and so on. Some people might think that making a schedule is a waste of time because they will take much time and extra effort for it. However, the more specified a schedule, the better to accomplish a goal [8]. Therefore, it is one of the most important parts in students' works for their research. Then, the system compares the schedule to data detected by sensors, and then the system gives some advice/notices to the user if the user falls behind on the schedule. If the user keeps to the schedule or runs ahead of the schedule, the system gives encouragement through praise. Moreover, each user and the professor share the data stored in the database for a long period. Even though every user is sure to know what they have done themselves so far, it is common for people to realize a fact how lazy their life style was after they look at their history of activities. Based on this history, the professor can also give proper advice to students. In addition, the system constantly monitors users' presence in each room so that laboratory members can grasp a situation of each member at real time. Therefore, the system can help smooth communication among students and between each student and a professor. And also, for visitors, to make them enjoy and feel convenience of a ubiquitous environment, the system provides services such as introduction of the laboratory and the announcement of the research achievements though moving images, sounds and texts.

- How to manage resources and documents in a laboratory

In a laboratory, there are a lot of resources such as books, journals, papers, hardware, software (i.e. CD-ROM), and the other things. However, it is hard to search who uses these resources, when and where users returned them, and so on. As is often the case, when a student wants to borrow a book or a device, the student can not find where it is. As a result, the student has to contact some of laboratory members to get it. In our research, RFID tags are attached to the items which is shared and also used frequently in a laboratory. By grasping the current location where these items are put, users can find an item they want whenever they access the system. This service also helps to prevent losing resources of a laboratory.

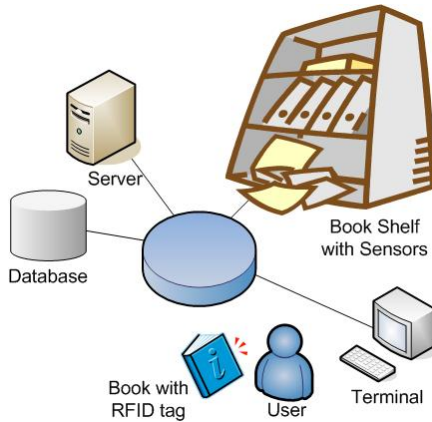


Fig. 3. Network Link of Book Shelf

In particular, to manage books on book shelves, we will apply the method of [9]. This research uses two infrared sensors to check whether a textbook is in or out from a school bag, and one RFID antenna to recognize which textbook is in/out. Each textbook is attached to a RFID tag with unique ID and book information. In our research, we embed two infrared sensors and one RFID antenna to one rack of a book shelf (see Fig. 3). Sensing a book by the infrared sensors and reading a RFID tag on the book, the system can immediately grasp which book is pulled out (borrowed) and which book is put on (returned) from the book shelf. The system saves a name of a book with time and a name of a person who borrows/returns the book to a database. Basically, the system gives support and advice through a terminal near the book shelf or an each user's PC. For example, if a student borrowing a book has not returned it for a quite long time, the system through a one's PC warns the student to return the book as soon as possible.

3 Comparing Method

To provide flexible and friendly service, the system should compare one data to the other data such as comparing a personal schedule to one's history of activities got from a sensor network as we mentioned in the previous section. Such a comparison between visible information is relatively easy. Meanwhile, a comparison between vague and invisible things like interests, knowledge levels, and preference is awkward. However, such a comparison is required for the system to give users detailed support.

Our method analyzes a similarity and a difference between objects and/or persons based on data from sensor networks by using the Euclidean distance. One example is to compare a similarity between an object and a person. U-Lab includes ubiquitous corner (U-corner) which introduces achievements of a laboratory to visitors. (Details of U-corner will be shown in the following section and also U-corner is implemented.) U-corner displays several exhibitions for visitors. Then the system introduces them as well as shows each visitor a suitable order to visit exhibitions.

At first, we set several parameters for a vector to every exhibition to decide the suitable path for a visitor. As an example, they can be education, hardware, matching,

and difficulty level. The values of these parameters are preset according to their research attribute. The range of each parameter is from one to five. The relationship goes closer the number becomes larger. For instance, Ubiquitous School Bag is an exhibition in the U-Corner. Considering its attribute, the vector will be set as (5, 3, 1, 3). Another example, a research of Matching between University Students in a Laboratory and Laboratory's OB/OG is an exhibition closely related with the education field, matching algorithm. Therefore, the vector may be set as (4, 1, 5, 2). On the other side, at the entrance, the system provides some simple questions to the visitor. These questions include several keywords related to those four parameters. Also, the system asks how long the visitor will stay in the U-Corner for coordinating the path and the number of exhibition should be shown to the visitor. Based on these questions, we can get a visitor's characteristic vector like the attribute vector of the exhibition. The range of the characteristic vector is also from one to five and each parameter has the same meaning to the attribute vector. By calculating the Euclidean distance between the characteristic vector and the attribute vector, we can get a result of their similarity. With these Euclidean distances, the system will generate a suitable, semantic visiting course for the visitor in the most interesting order. Following are some definitions and a formula for Euclidean distance calculation.

$$\vec{A}_i = \begin{pmatrix} A_{i0} \\ A_{i1} \\ \vdots \\ A_{in} \end{pmatrix} \text{ And } \vec{C}_j = \begin{pmatrix} C_{j0} \\ C_{j1} \\ \vdots \\ C_{jn} \end{pmatrix}. \quad (1)$$

The above denotes an attribute vector of an exhibition and a characteristic vector of a visitor respectively. Note that each component of the vectors is from one to five.

Let d_{ij} denotes the Euclidean distance between a certain attribute vector and a certain characteristic vector which is calculated by the following.

$$d_{ij} = \sqrt{\sum_{a=0}^n (A_{ia} - C_{ja})^2}. \quad (2)$$

The system will sort the distances in a shortest path first algorithm and guide the visitor to the exhibition which is most matching with the visitor. Also, the system will generate a boundary value from the question, limitation of the tour time, we mentioned above to adjust how many exhibitions should be shown to the visitor.

4 Implementation

4.1 Model of Ubiquitous Corner

In recent years, national and public universities are turned into independent administrative entities in Japan. Under the influence of this trend, business-academia

collaboration takes an important role more and more than before. In that way, an open laboratory would be a key event of all in a university. In this research, as we mentioned in the previous section, we implemented a U-Corner as a representative example of the ubiquitous laboratory. U-Corner is a space which introduces achievements of the laboratory to visitors. The ubiquitous corner is included in the ubiquitous laboratory.

In this research, the whole space of the corner can detect people’s actions based on a sensor network. The sensor network is composed of two or more pressure sensors, infrared sensors and RF-ID readers. Every visitor will be given a RFID tag at the reception desk to enjoy the ubiquitous environment. The tag stores his/her information, such as occupation, interests, visiting history, visiting path. It is supposed that the tag is attached to the visitor when he/she is in the ubiquitous corner. The following section will describe the definition of the U-Corner and classify the results of research achievements.

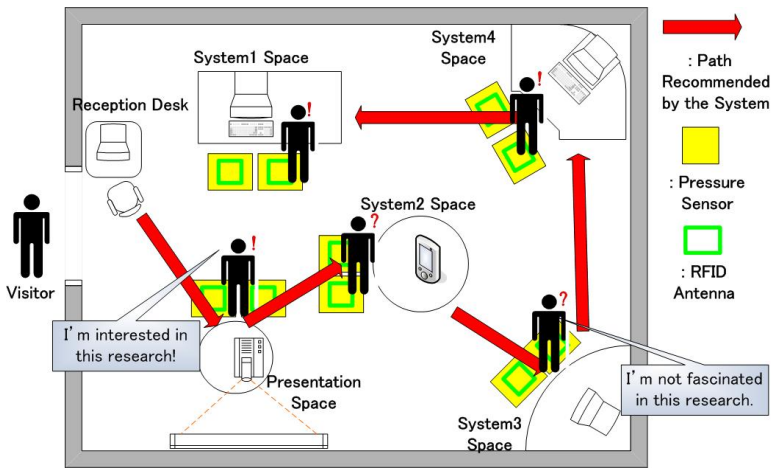


Fig. 4. The Model of the Ubiquitous Corner

Fig. 4 shows a floor plan of the U-Corner. There are many exhibitions in it. Each exhibition shows one of the research achievements. The floor of the ubiquitous corner is filled with some special tiles which includes pressure sensors and RF-ID antennas. RF-ID antennas can detect the identity of the visitor and pressure sensor can know the current place of the visitor. The antennas and pressure sensors are controlled by a relay circuit (a logical disjunction circuit) because each tile has more than one antenna and pressure sensor. Through the circuit, the system can know the identity and location information of the visitor. When a visitor enters in the U-Corner, he/she will be given support to experience a ubiquitous environment. At first, the visitor will be asked some questions about his/her interesting, occupation and so on. Then, the system will show a suitable visit path to the learner based on the result of an analysis of his/her input information.

4.2 Interaction with the Special Tile

After the visitor entered the U-Corner, the system always checks the position where the visitor is. When the visitor watches an exhibition, he/she can have some interaction with the tiles. If he/she find the exhibition is interesting, he/she can step the right tile to let system know his/her feeling. If not, he/she can step the left tile. Then, based on our method, the system will recalculate the path for next seeing. As we explained in the section 4, our idea is to adjust the characteristic vector to bring the two vectors more closely or more far. If the visitor shows interesting in the exhibition, the system will reinforce the similarity in current direction. If not, the system will reduce the parameters. The system will compare every parameter between two vectors.

- Interesting Case


```
for(k=-0; k<=n; k++) {
  If (Aik < Cjk)   Cjk = Cjk - 1;
  If (Aik == Cjk)  Cjk = Cjk;
  If (Aik > Cjk)   Cjk = Cjk + 1;
}
```
- None Interesting Case


```
for(k=-0; k<=n; k++) {
  If (Aik > Cjk)   Cjk = Cjk - 1;
  If (Aik <= Cjk)  Cjk = Cjk + 1;
}
```

Table 1. An Example of Two Vectors

| Attribute Vector | A _{i0} | A _{i1} | A _{i2} | A _{i3} |
|-----------------------|-----------------|-----------------|-----------------|-----------------|
| \vec{A}_i | 1 | 3 | 5 | 2 |
| Characteristic Vector | C _{j0} | C _{j1} | C _{j2} | C _{j3} |
| \vec{C}_j | 4 | 1 | 2 | 3 |

Table 1 is an example to explain the algorithm. Suppose a certain exhibition's attribute vector is (1, 3, 5, 2) a certain visitor's characteristic vector is (4, 1, 2, 3). Based on the algorithm, if the visitor shows interesting on the exhibition, the visitor's characteristic vector will be replaced by (3, 2, 3, 2). On the other hand, it will be (5, 1, 1, 4). After the calculation, the system will use a revised one to give a next guidance.

4.3 Difficult Points of Development

The most difficult point of development was how to capture the visitor's action; where they are? And which exhibition they are watching?

To solve this problem, we proposed a tile to detect visitor's action (See Fig. 5). It is composed of a RF-ID antenna and pressure sensors. Passive RF-ID reader [10] only has a narrow range of operation. The antenna and reader are combined by default. Sometimes it works not well for gathering visitor's action. We separated the antenna from the

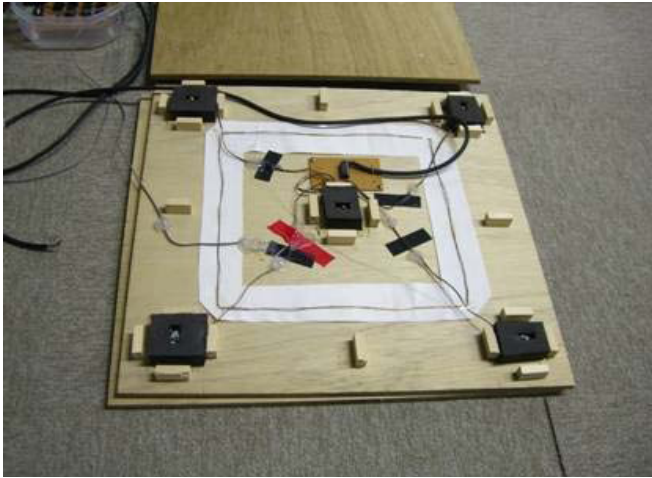


Fig. 5. A Tile for Gathering Visitor's Action

reader and created a RF-ID antenna with coil to broad the operation range of it. As the result, with a relay circuit 16 antennas can control by only one reader. The tile also has five pressure sensors. Each one is buried in a sponge and some chips are around the sponge to protect the sensor from weight of the visitor. By using the special tile, accuracy of gathering visitor's movement was increased.

5 Experiment and Verification of the System

The purpose of experiment shows the followings.

1. Could the system know the visitors interesting?
2. Is the support suitable for visitors?
3. Is the system useful for LAB introducing?

These three points are examined through the experiment. We got 15 students' corporations to execute this experiment. First, they registered at the entrance to initialize their personal information. Also, each one held a RF-ID tag in this experiment. During their visiting, they interacted with the special tile and experienced some support. After the experiment, we asked them to answer several questions.

- Q1. Could this system have guided exhibitions according to your interest?
- Q2. Was the support of this system appropriate?
- Q3. Was the system useful for introducing the laboratory?
- Q4. Was a ubiquitous environment able to be experienced through this system?

The result of experiment can be explained as follows. 75% people feel the guide is done according to their interesting. This data indicate the path making algorithm still leave room for improvement. In contrast, about 40% visitors think the support provided by the system is not so appropriate. The timing of support, the way of support should be

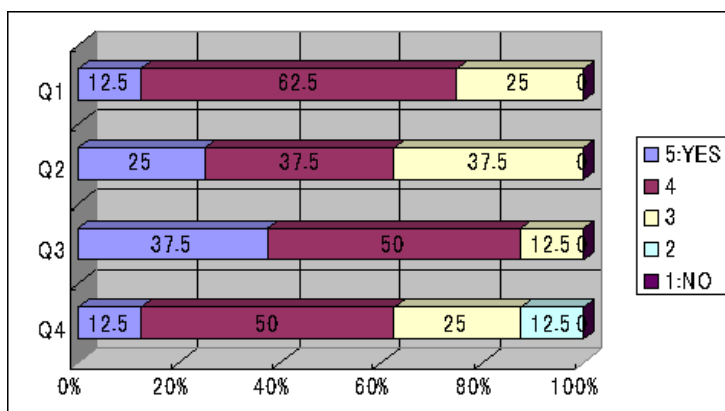


Fig. 6. The Result of Experiment

discussed in the future. The result of Q3 shows that it is a useful way to guide a visiting path for laboratory introduction. 62.5% of visitors think they experienced a ubiquitous environment in the U-Corner. This can be progressed by changing the way to collect visitors' interesting not by asking question but by analyzing their action. Also, the interaction with the tile can have more variation.

6 Conclusion and Future Work

In this paper, we designed a ubiquitous environment based on an existing laboratory to support college students, professors, and visitors using sensor network. To provide flexible and friendly service, we proposed an analyzing method by using the Euclidean Distance. As the case study of the whole U-Lab, we implemented a ubiquitous corner which provides a guide system to laboratory visitors based on their interesting. Through the experiment, the results show it is useful for laboratory introduction with a ubiquitous environment. Our proposal is revealed useful and practical.

In the next step, we will implement the whole ubiquitous laboratory. Also, some problems found in the experiment will be solved. More sensors, such as light sensor, temperature sensor, acceleration sensor can be added to the tile to get more information about people.

References

1. School of Human Sciences, Waseda University: E-School, <http://e-school.human.waseda.ac.jp/>
2. Oklahoma State University: Online Courses, <http://oc.okstate.edu/>
3. Taniguchi, R.: Development of a Web-based CAI System for Introductory Visual Basic Programming Course. Japanese Society for Information and Systems in Education 19(2), 106–111 (2002)

4. Fuwa, Y., Nakamura, Y., Yamazaki, H., Oshita, S.: Improving University Education using a CAI System on the World Wide Web and its Evaluation. *Japanese Society for Information and Systems in Education* 20(1), 27–38 (2003)
5. Korkea-aho, M.: Context-Aware Applications Survey (2005), <http://users.tkk.fi/mkorkea/doc/contextaware.html>
6. Cheng, Z., Sun, S., Kansen, M., Huang, T., He, A.: A Personalized Ubiquitous Education Support Environment by Comparing Learning Instructional Requirement with Learner's Behavior. In: *AINA* (2005)
7. Helal, A., Mann, W., Elzabadani, H., King, J., Kaddourah, Y., Jansen, E.: Gator Tech Smart House: A Programmable Pervasive Space. *IEEE Computer Magazine*, 64–74 (2005)
8. Shimamune, S.: *Performance Management: Behavior Analysis for Solving Problems*, 5th edn. Yoneda Publisher, Inc., Chiba (2000)
9. A Smart Schoolbag System for Reminding Pupils of the Forgotten Items
10. D.T.K Ltd., <http://zones.co.jp/mezam.html>
11. Srivastava, M., Muntz, R., Potkonjak, M.: Smart kindergarten: sensor-based wireless networks for smart developmental problem-solving environments. In: 7th annual international conference on Mobile computing and networking, pp. 132–138 (2001)
12. Barbosa, J., Hahn, R., Barbosa, D.N.F., Geyer, C.F.R.: Mobile and ubiquitous computing in an innovative undergraduate course. In: 38th SIGCSE technical symposium on Computer science education, pp. 379–383 (2007)
13. Brunette, W., Lester, J., Rea, A., Borriello, G.: Some sensor network elements for ubiquitous computing. In: 4th international symposium on Information processing in sensor networks, article no. 52 (2005)

Intelligent Monitoring Using Wireless Sensor Networks

Senol Zafer Erdogan¹, Sajid Hussain², and Jong-Hyuk Park³

¹ Faculty of Engineering, Maltepe University, Istanbul, Turkey
senole@maltepe.edu.tr

² Jodrey School of Computer Science, Acadia University, Wolfville, Canada
Sajid.Hussain@acadiau.ca

³ Department of Computer Engineering, Kyungnam University, Masan, Korea
parkjonghyuk@gmail.com

Abstract. Wireless sensor networks (WSNs) enable smart environments to provide pervasive and ubiquitous applications, which give context-aware and scalable services to the end users. In this paper, an agent-based architecture is proposed for knowledge discovery and the variation in received signal strength indicator (RSSI) is used for knowledge extraction. Several experiments are conducted in an in-door environment to demonstrate the application of RSSI for ubiquitous monitoring. For instance, a WSN, which consists of Moteiv's Tmote Sky sensors, is deployed in a bedroom to determine the sleeping behavior and other physical activities of a person. Similarly, a WSN is used to identify the occupied chairs in a room, as well as the mobility of a person.

1 Introduction

A smart environment can be created by using dense deployment of sensors to provide in-situ and precise monitoring, as well as using actuators to enable real-time, adaptive, and context-aware control mechanisms.

WSNs consist of a large number of smart sensors that have limited computing, storage, communication, and energy resources. These smart devices can interact with one another to create self-organized, ad hoc, and scalable networks that can provide intelligent, pervasive, and ubiquitous applications [1]. For example, sensors networks are used in military, security, health-care [2], environment and habitat monitoring. Further, as computing, storage, and communication resources are very limited for current available sensors, there is a need for energy efficient algorithms and techniques to provide scalable solutions [3].

As RSSI values vary because of mobility and obstruction, the RSSI variation can be used in the investigation of localization and mobility. Further, as the variation in RSSI values is non-uniform and non-deterministic with respect to distance and time, the simulation studies are not sufficient. As a result, the deployment environment should be investigated with real WSN experiments. In this paper, several experiments are conducted using Moteiv's Tmote Sky sensors to study the behavior of RSSI values for localization and mobility of a person in an in-door environment. The experiment results confirm that the variation

in RSSI values can be used for localization and mobility. For example, sensors deployed in a bed room are used to determine the following: a) time spent at the study table, b) time spent on a bed, and c) wake-up time. Similarly, in a classroom environment, RSSI values are used to identify the occupied chairs, as well as the duration the chairs were occupied.

The remaining paper is organized as follow: Section 2 gives a brief description regarding RSSI related research. Section 3.1 describes an architecture for a smart application. Section 4 provides the experiment details and results. Finally, Section 5 concludes the paper.

2 Related Work

There is an active research in estimating the values of RSSI, link quality indicator (LQI), and packet reception rate (PRR) for realistic radio communication [4], [5], [6], [7], [8]. Zhou et al. [4] investigate the degree of variation in RSSI values and propose a non-circular radio irregularity model (RIM) for sensor networks. Gallais et al. [9] discuss the effect of a realistic radio channel on area coverage protocols. Scott et al. [10] use transmit and receive signal strengths to investigate propagation patterns. Halkidi et al. [11] use an online mechanism to determine the overall network status and to reduce the communications costs.

Erdogan and Hussain [12] investigate radio irregularity with respect to distance, sending power level, direction, and alignment of the sensor node from the base station. The experimental results show that proper alignment and sending power level can reduce the energy consumption, in order to increase the network lifetime. In this paper, however, the focus is not on reduced energy consumption but the objective is to extract knowledge and context information from the RSSI values. The variance in RSSI values can be used to identify user behavior, mobility, and environment.

RFID tags are commonly used for precise object tracking and inventory control [13] [14]; however, these tags could be inconvenient for general human usage because RFID tags must be attached to a person. Sensor motes, on the other hand, can be used to detect mobility or user behavior without any wiring or a tag attached to a person. Certainly, the sensor motes cannot provide the exact identification accuracy as of RFID tags; however, in several applications, we do not need the exact identification. The sensor motes can provide unobtrusive monitoring at common places such as hospitals, restaurants, homes, schools, and offices. Further, the sensor motes can also help in maintaining person's privacy. Although the information about the behavior of a person would be known, it would be relatively easy to hide the person's identity.

3 Architecture

3.1 Terms and Definitions

As the RSSI values vary with respect to the deployment environment, we describe a few terms that would be needed in the investigation of RSSI.

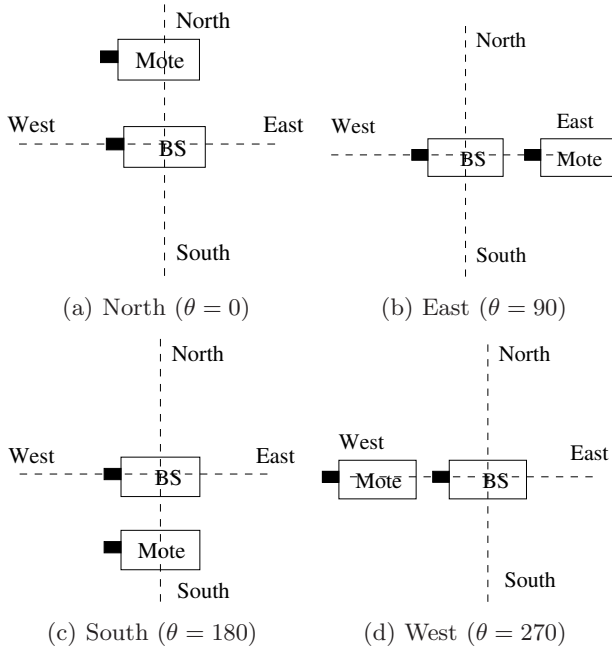


Fig. 1. Directions for node placements

Definition 1. Direction θ is defined as the angle with respect to the geographical direction, where North, East, South, and West are considered as 0, 90, 180, and 270 respectively.

Direction is used to identify the physical location of a node with respect to a given node. Figure 1 illustrates some of the examples where a node can be placed. For instance, Figure 1(a) shows that a node is placed at North direction ($\theta = 0$) with respect to the base station. Similarly, Figure 1(b), Figure 1(c), and Figure 1(d) show that nodes are placed at East, South, and West directions respectively. Further, we can use angle to identify the location. The angle starts from North direction and continues in clockwise direction. For example, the directions of nodes placed at North, East, South, and West can be represented as $\theta = 0$, $\theta = 90$, $\theta = 180$, and $\theta = 270$.

Definition 2. Alignment γ is defined as the angle between two motes.

Figure 2 shows different alignments for a sensor mote. Figure 2(a) and Figure 2(b) show sensor motes that are in North ($\theta = 0$) direction but alignments are $\gamma = 0$ and $\gamma = 90$ respectively. However, motes in Figure 2(b) and Figure 2(c) have same alignment ($\gamma = 90$) but their directions are North ($\theta = 0$) and East ($\theta = 90$) respectively.

Definition 3. Distance d is as defined as a Euclidean distance between two motes.

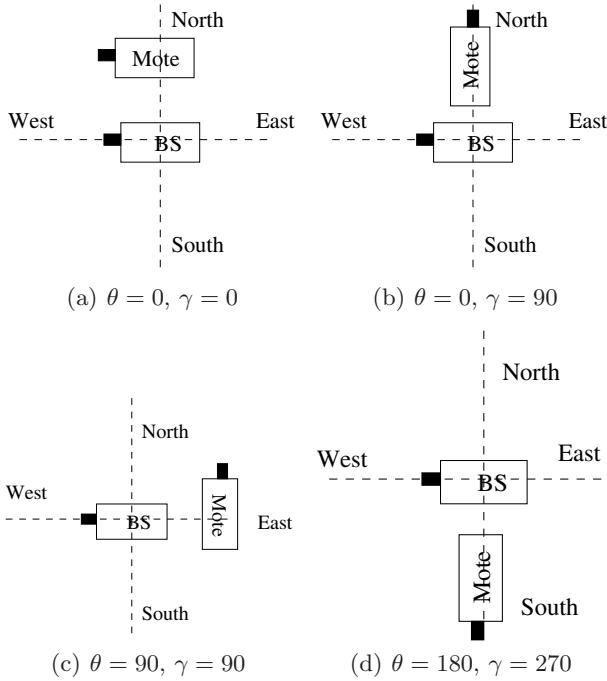


Fig. 2. Alignment of sensor motes

The distance d can be measured directly between two motes or can be computed from their co-ordinates, as shown below:

$$d = \left| \sqrt{|y_2 - y_1|^2 + |x_2 - x_1|^2} \right| \tag{1}$$

Distance is commonly used in localization techniques based on RSSI estimation; however, the distance d parameter should be combined with direction θ and alignment γ parameters for accurate investigation of deployment environment. For instance, in many radio communication models, energy consumption is considered as directly proportional to the square of distance (circular model) [15], which is not applicable in most of the realistic environments. As a result, change in RSSI ($\Delta RSSI$) is a function of the above parameters:

$$\Delta RSSI = f(\theta, \gamma, d) \tag{2}$$

Further, the above equation is valid for static environment only. For dynamic or mobile environments, RSSI will also vary with respect to time, as given below:

$$\Delta RSSI = f(\theta, \gamma, d, t) \tag{3}$$

For instance, if sensors are mobile or if there are other moving objects in the neighborhood, RSSI will vary with respect to time, as given in Equation 3.

An architecture for a WSN application to provide knowledge discovery and data mining would contain the following:

- A base station (BS) to connect the sensor network to traditional networks.
- A service agent that would contain the following entities: a) a communication component to abstract the communication details of the application, b) database component to store the data retrieved from the WSN, c) knowledge component to extract knowledge from the data stored in a database, and d) context-aware services for the application users. As service agent needs extensive computing and storage resources, it must be located on a computer or a gateway node.
- Sensor nodes to provide in-situ monitoring.
- WSN agents would be located at sensor nodes. Although the WSN agents would have similar components as a service agent; the WSN agent's components would provide minimal functionality because of limited resources of the sensor.
- An application (say Web application, Web App) to provide customized services to the end users.

Figure 3 shows the proposed agent-based architecture for the knowledge discovery application. The base station acts as a bridge between sensor network and the regular network. The application contains a service agent that can provide several context-aware services. The service agent contains the following entities: a communication component, database, and a knowledge extraction component. The communication component interacts with the external entities, such as base station. The communication component is connected to both knowledge component and database. All the incoming data is directly stored in a database for offline processing and stable storage. Further, the communication component is directly connected to the knowledge component, in order to provide real-time analysis and services. The service agent provides a given number of context-aware services to the subscribed users or applications. A web application, for instance, can use these context-aware services to provide customized web pages to the end user. Moreover, each sensor contains a sensor agent that has features

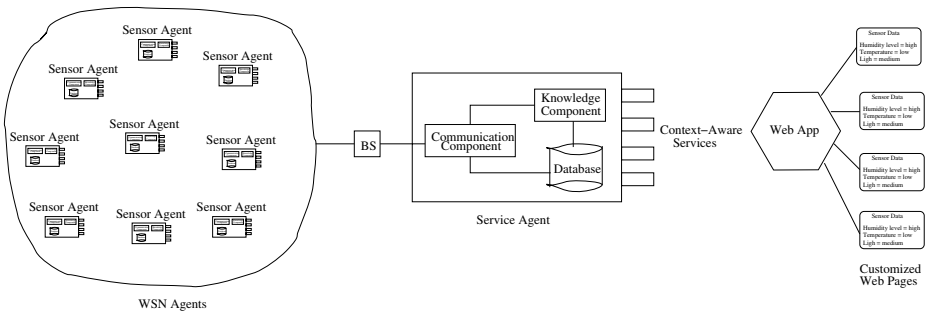


Fig. 3. Agent-based Architecture for Smart Applications

identical to service agent; however, the sensor agent has minimal functionality because of limited computing and energy resources of sensors.

Service agent's knowledge component extracts non-trivial information from the incoming data stream. For instance, for a WSN deployed in a bedroom environment, the variation in the variance of RSSI values can be used to identify the sleeping behavior, study habits, and physical activities of a person.

4 Experiment Results

Experiments are conducted in an in-door environment to investigate localization and mobility of a person. The variance in RSSI values is used to identify the current location and activities of a person.

4.1 Localization Example

Figure 4 shows the experimental setup for a localization example. The sensors are deployed on 4 tables to identify any activity near the tables. The variation in RSSI values is used to determine the mobility or activity near a table. The experiment details are as follows:

- Base station is in the center of the room.
- There are 4 pairs of table and chair in four corners of the room. The distance between horizontal (along X-axis) tables is 7.8 m and the distance between vertical (along Y-axis) tables is 5 m.
- Moteiv's Tmote Sky¹ sensors are used for the base station and the 4 sensor motes.
- The time span for one experiment is 7 minutes. For confidence, the same experiment is conducted for 3 times.
- One person alternately sits on all the chairs.

The sensor motes send a packet to the base station after every second. For an occupied chair, the variance in RSSI values will be significantly different as compared to unoccupied chairs. As a result, the RSSI variance is used to identify the location and mobility of a person.

Figure 5 shows the RSSI values for 7 minute time interval (approximate) for all motes. Figure 5(a) shows RSSI values for a mote that is near Chair 1. Since Chair 1 is occupied during 1-65 seconds, there is relatively high variation in RSSI values. In other words, the high variation can determine the chair occupancy. However, during the same time interval, the RSSI values for mote 2, mote 3 and mote 4 are almost constant. Thus, it can be assumed that unoccupied chairs have relatively low variation in RSSI values. Similarly, Figure 5(b), Figure 5(c), and Figure 5(d) show the RSSI values for motes near Chair 2, Chair 3, and Chair 4 respectively. As expected, for all motes, the variation in RSSI values is relatively high for occupied time interval as compared to unoccupied duration, when the chair is unoccupied. The above experiment determines the following:

¹ <http://www.moteiv.com>

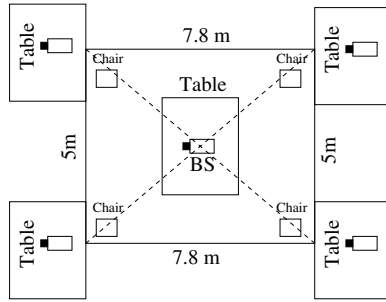


Fig. 4. Room Layout for the Localization Experiment

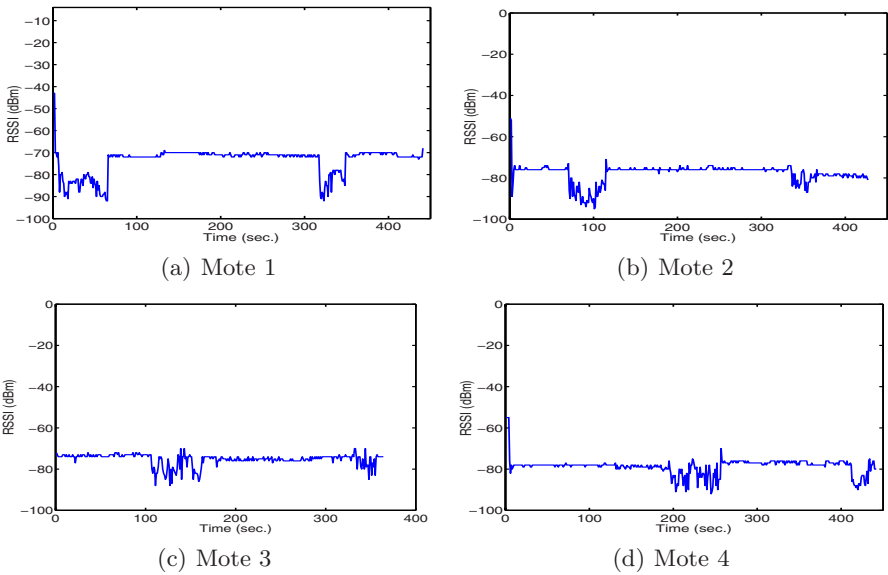


Fig. 5. RSSI variation for 4 motes

- Each chair was occupied for a some period of time.
- At one time, only one chair was occupied.
- There is a rapid (or spontaneous) activity in moving from one chair to the next.

Table 1 shows the variance in RSSI values for different time intervals. As three experiments are conducted, the variance of each experiment is given for each mote. The results confirm the observation that variance in RSSI values can determine the occupied chair. For instance, for time interval 1-65 seconds, when chair 1 is occupied, the variance in Mote 1 is significantly high as compared to the remaining time intervals when the Mote 1 was unoccupied. Similarly, variation

Table 1. Variance in RSSI values for Motes

| Time (sec.) | Variance in RSSI values | | | | | | | | | | | |
|-------------|-------------------------|-------------|-------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| | Mote 1 | | | Mote 2 | | | Mote 3 | | | Mote 4 | | |
| | Exp 1 | Exp 2 | Exp 3 | Exp 1 | Exp 2 | Exp 3 | Exp 1 | Exp 2 | Exp 3 | Exp 1 | Exp 2 | Exp 3 |
| 1-65 | 50.8 | 45.3 | 48.1 | 0.37 | 1.24 | 1.53 | 0.49 | 0.94 | 1.12 | 0.46 | 0.59 | 1.13 |
| 66-130 | 0.26 | 0.84 | 1.23 | 44.46 | 48.63 | 39.32 | 1.96 | 2.34 | 1.70 | 0.1 | 1.02 | 0.83 |
| 131-190 | 0.17 | 0.46 | 0.79 | 0.20 | 0.89 | 1.93 | 15.18 | 17.43 | 17.21 | 0.55 | 0.79 | 0.94 |
| 191-260 | 0.35 | 0.22 | 0.54 | 0.49 | 0.94 | 1.03 | 0.53 | 1.21 | 0.93 | 23.10 | 29.62 | 31.42 |

in RSSI variances is high for motes 2, 3, and 4 when their corresponding chairs are occupied.

The above experiment can be used in the following applications:

- Industrial exhibition: popular information posters, displays, or demos can be determined.
- Restaurants: the unoccupied tables, as well as popular tables can be identified.
- Parking: the available parking spots.

In another experiment, two sets of tables and chairs are used. A person alternately sits on a chair for 5 minute time interval. The distance between two tables is 5m. Figure 6 shows variation in RSSI values for both motes. As shown in Figure 6(a) and Figure 6(b), the variation in RSSI values can determine the occupied chair. For instance, in time interval 1-5 minutes (300 seconds), table 1 is occupied and table 2 is unoccupied. However, in time interval 6-10 minutes (300 - 600 seconds), table 2 is occupied and table 1 is unoccupied.

The above results can be used to develop WSN-based localization and context-aware services. For instance, in a museum or an art gallery environment, the time spent by visitors on a specific master-piece can be determined by the above

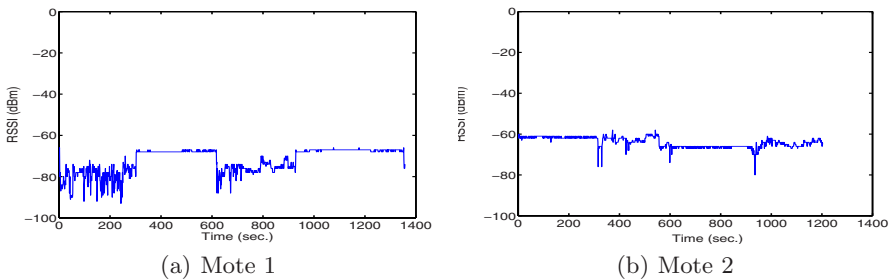


Fig. 6. RSSI variation for 2 motes with 2 tables

experiment. Similarly, the above experiments can also be used to identify the popular booths or demos in an industrial or art exhibition.

4.2 Monitoring Human Behavior in a Bedroom

In this experiment, sensors are deployed in a bedroom to monitor the behavior, mobility or lifestyle of a person. For instance, the sensors can be used to determine the time spent on the study table or on a bed.

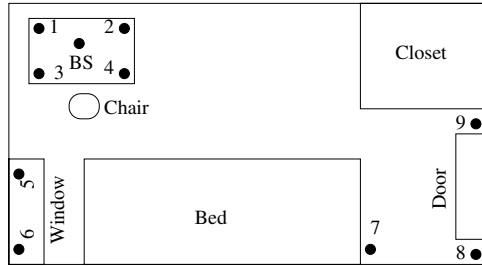
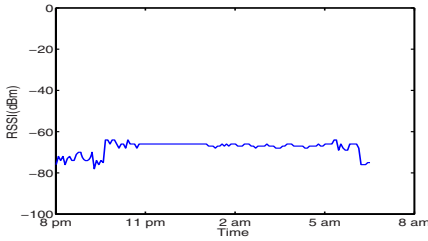


Fig. 7. Room plan of a bedroom

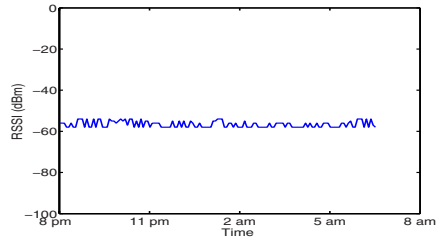
Figure 7 shows the room plan of a bedroom. The sensors are deployed as follows: 4 sensors on a study table (Mote 1, Mote 2, Mote 3, and Mote 4), 2 sensors near the window (Mote 5 and Mote 6), 1 sensor on the corner of bed (Mote 7), and 2 sensors near the door (Mote 8 and Mote 9). The base station is attached to a laptop on the study table. The sensor data is collected for several days.

Figure 8 shows RSSI values for table, window and door sensors. RSSI variation confirms with the actual behavior of a person. For instance, as recorded by the person, the RSSI variation confirms the behavior observed by the sensors. The student was working at the study table for the initial 3 hours, which is confirmed by RSSI variation for Table motes 1 and 3, as shown in Figure 8(a) and Figure 8(c) respectively. Further, the small variation for Table motes 2 and 4 (Figure 8(b) and Figure 8(d)) indicates that the person's sitting position did not affect these values. By comparing the RSSI values of Table motes 1, 2, 3, and 4, the sitting posture or inclination on a table can also be determined, although it is not investigated in this paper.

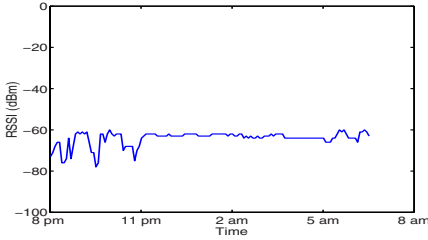
After 3 hours of working, the person slept for 7-8 hours. The sleeping time is also evident from RSSI values of window and door motes. Further, the RSSI variation for door motes are not consistent. For instance, Mote 8 (Figure 8(g)) near the bed confirms the sleep behavior; however, the mote near the closet (Mote 9) shows some unexpected RSSI variation. Finally, the RSSI variation in the last couple of hours shows the morning activity, which is confirmed by most of the motes.



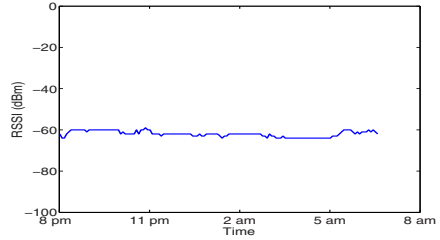
(a) Table: Mote 1



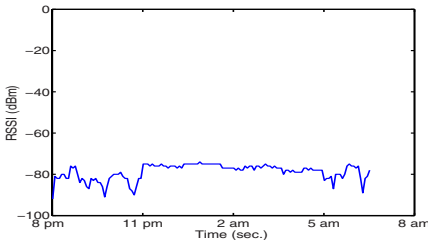
(b) Table: Mote 2



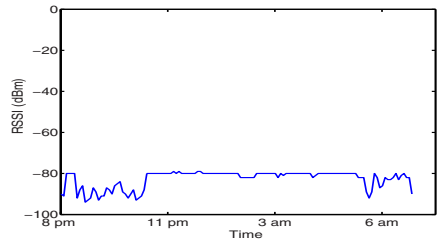
(c) Table: Mote 3



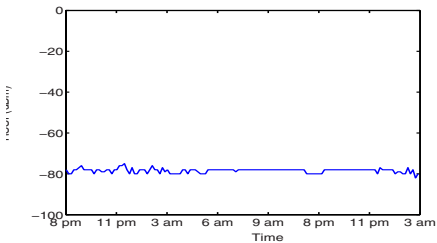
(d) Table: Mote 4



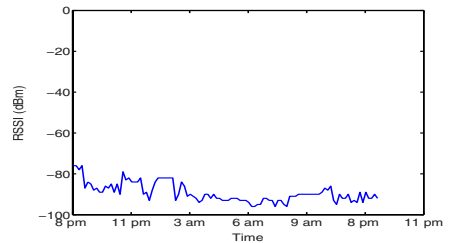
(e) Window: Mote 5



(f) Window: Mote 6



(g) Door: Mote 8



(h) Door: Mote 9

Fig. 8. RSSI variation for sensors in a bedroom

The above results can be used in maintaining a daily activity diary for a person. The results obtained at the base station can be logged in a database and can be retrieved through a web-based application. Consequently, a life style of a person, active or sedentary, can be estimated by these results.

5 Conclusion and Future Work

In this paper, an agent-based architecture is proposed for knowledge discovery. The variation in RSSI values is used for knowledge extraction. Several experiments are conducted in an in-door environment such as: a) a WSN is deployed in a bedroom to determine the sleeping behavior and other physical activities of a person, b) a WSN is used to identify the occupied chairs in a room, as well as the mobility of a person, and c) humidity sensor of Moteiv's Tmote Sky is used for knowledge extraction.

In future, the fuzzy-based logic and other machine learning techniques will be used for knowledge discovery and data mining. Further, the context-aware services and end-user applications will be provided.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on wireless sensor networks. *IEEE Communication Magazine* (2002)
2. Gao, T., Greenspan, D., Welsh, M., Juang, R.R., Alm, A.: Vital signs monitoring and patient tracking over a wireless network. In: *The 27th Annual International Conference of the IEEE EMBS, Shanghai, China* (2005)
3. Kahn, J., Katz, R., Pister, K.: Next century challenges: Mobile networking for smart dust. In: *MobiCom 1999. The ACM International Conference on Mobile Computing and Networking, Seattle, USA* (1999)
4. Zhou, G., He, T., Krishnamurthy, S., Stankovic, J.A.: Impact of radio irregularity on wireless sensor networks. In: *MobiSys. The International Conference on Mobile Systems, Applications, and Services, Boston, USA* (2004)
5. Gu, L., Jia, D., Vicaire, P., Yan, T., Luo, L., Tirumala, A., Cao, Q., He, T., Stankovic, J.A., Abdelzaher, T., Krogh, B.H.: Lightweight detection and classification for wireless sensor networks in realistic environments. In: *The 3rd ACM Conference on Embedded Networked Sensor Systems, San Diego, USA* (2005)
6. Cerpa, A., Busek, N., Estrin, D.: Scale: A tool for simple connectivity assessment in lossy environments. In *CENS Technical Report 0021* (2003)
7. Ganesan, D., Krishnamachari, B., Woo, A., Culler, D., Estrin, D., Wicker, S.: Impact of radio irregularity on wireless sensor networks. In *Technical Report UCLA/CSD-TR 02-0013* (2002)
8. Woo, A., Tong, T., Culler, D.: Taming the underlying challenges of reliable multi-hop routing in sensor networks. In: *SenSys 2003, Los Angeles (USA)* (2003)
9. Gallais, A., Parvery, H., Carle, J., Gorce, J.-M., Simplot-Ryl, D.: Efficiency impairment of wireless sensor networks protocols under realistic physical layer conditions. In: *ICCS 2006. 10th IEEE International Conference on Communication Systems, Singapore* (2006)
10. Scott, T., Wu, K., Hoffman, D.: Radio propagation patterns in wireless sensor networks: New experimental results. In: *IWCMC 2006. IEEE International Wireless Communications and Mobile Computing Conference, Vancouver, Canada* (2006)
11. Halkidi, M., Kalogeraki, V., Gunopulos, D., Papadopoulos, D., Zeinalipour-Yazti, D., Vlachos, M.: Efficient online state tracking using sensor networks. In: *MDM 2006. The 7th International Conference on Mobile Data Management* (2006)

12. Erdogan, S., Hussain, S.: Experiences in realistic radio communication for wireless sensor networks. Technical Report, Jodrey School of Computer Science, Acadia University, TR-2007-002 (2007)
13. Vogt, H.: Efficient object identification with passive rfid tags. LNCS. Springer, Heidelberg (2002)
14. De, P., Basu, K., Das, S.K.: An ubiquitous architectural framework and protocol for object tracking using rfid tags. In: MOBIQUITOUS. The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (2004)
15. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the Hawaii International Conference on System Sciences (2000)

On the Design of Micro-mobility for Mobile Network*

Junn-Yen Hu¹, Chen-Fu Chou², Min-Shi Sha²,
Ing-Chau Chang³, and Chung-Yi Lai⁴

¹ Graduate Institute of Networking and Multimedia

² Department of Computer Science and Information Engineering
National Taiwan University, Taiwan, R.O.C.

{sysrq, ccf, minshi}@cmlab.csie.ntu.edu.tw

³ Department of Computer Science and Information Engineering
National Changhua University of Education, Taiwan, R.O.C.

icchang@cc.ncue.edu.tw

⁴ Institute for Information Industry, Taiwan, R.O.C.

laici@iii.org.tw

Abstract. The micro-mobility issue has been discussed in host mobility in the past decade while the network mobility has become increasingly popular recently. Hence we believe that developing a micro-mobility scheme for mobile network is important and a micro-mobility scheme called Micro-NEMO is proposed in this work. The Micro-NEMO can provide local movement within an administrative domain for a moving network and be compatible with NEMO basic support protocol since it is extended from HMIPv6. Furthermore, we develop an enhanced Micro-NEMO to solve the pinball routing problem. The simulation results indicate that Micro-NEMO and its enhanced scheme can achieve a better performance than other mobility schemes in terms of number of binding update, average handoff latency, end to end delay and packet overhead.

Keywords: Mobile Network, Network Mobility, Mobility Management, Micro-mobility, Mobile Router, HMIPv6.

1 Introduction

The deployment of wireless networks has made mobility management research field more important. The state of the art on mobility management has been categorized into macro-mobility and micro-mobility, which could be differentiated by distinct types of handoff procedure of a mobile host. Macro-mobility means that a large scale of movement of a mobile across diverse administrative domains. C.E. Perkins purposed the Mobile IP (MIP) [1, 2] which has become the major scheme for macro-mobility. This scheme represents a simple and scalable global mobility solution while a mobile host is moving. However, the macro-mobility scheme is not suitable for

* This work was partially supported by the National Science Council and the Ministry of Education of R.O.C. under the contract No. NSC95-2221-E-002-103-MY2 and NSC95-2622-E-002-018.

Table 1. Current state of the art for mobility management

| | Host mobility | Network mobility |
|----------------|---|-----------------------------|
| Macro-mobility | Mobile IP | NEMO Basic Support Protocol |
| Micro-mobility | Hierarchical Mobile IP, Cellular IP, HAWAII, etc. | Currently none |

movement in a small scale domain or at a high speed movement because it might incur a lot of global registration procedures and this could lead to heavy signaling overheads and significant performance degradation, e.g., the handoff latency. In order to improve the performance for mobile internet users, the micro-mobility concept was purposed. Micro-mobility means that local movement of a mobile within an administrative domain. Several Protocols such as Hierarchical Mobile IP (HMIP) [3], Cellular IP (CIP) [4, 5], HAWAII [6] have been proposed for micro-mobility. This kind of protocol has the benefit of eliminating registration between mobile host and possibly distant home agent (HA) and reducing handoff latency when the mobile node is still inside same identical local coverage area. To support mobile internet users, integration of macro- and micro-mobility can achieve objectives of low handoff latency and minimal signaling cost.

In addition, differentiated by distinct types of handoff procedure, mobility management still can be discussed from the view point of number of moving mobile hosts. If the subject of discussion is about a single mobile host moving, it is called host mobility. If a set of users are moving together via a certain transportation carriage, e.g., a bus, a train, or an aircraft, the transportation carriage can be regarded as a mobile network. This type of mobility is referred to the network mobility and the moving network is called mobile network [7]. The Internet Engineering Task Force (IETF) has proposed a basic protocol for the mobile network, named Network mobility (NEMO) basic support protocol [8], to support a large scale movement of a mobile network. In NEMO, a mobile router (MR) is able to manage the mobility of a set of mobile hosts within the same mobile network. Thus, mobile hosts inside the moving network should not perceive that MR changes point of attachment and the binding update storm can be avoided. In addition, a MR might allow other MRs to associate with itself, i.e., one mobile network could get on another mobile network. This is referred to nested NEMO, which might suffer from the pinball routing problem (so-called ‘dog-leg problem’).

The current state of the art for mobility management is described in Table 1. We note that many works discussed with micro-mobility issue in host mobility but did not in network mobility area. Many previous works aim to cope with the pinball routing problem of network mobility without focusing on micro-mobility issue. On the other hand, several works are not compatible with NEMO and support VMN that gets off the vehicle. We believe that micro-mobility issue in network mobility is worth discussing because the vehicle might perform many local movements such as a car move inside a city or a campus. Hence, we propose a scheme called Micro-NEMO (Micro-mobility scheme for mobile network) in this paper.

To support micro-mobility issue for the network mobility scheme, our Micro-NEMO scheme could provide that a vehicle can be local movement of micro-mobility and that visiting mobile node (VMN) still can perform micro-mobility if it gets off the vehicle. In other words, our scheme is able to efficiently integrate both network mobility and micro-mobility concepts. In addition, Micro-NEMO scheme is compatible with NEMO and host micro-mobility (for VMN get off a vehicle). Furthermore, to deal with the pinball routing problem, we provide an enhanced Micro-NEMO, which is able to perform the procedure of route optimization. Simulation results have showed that Micro-NEMO and enhanced scheme are able to improve the number of binding update, average handoff latency, end to end delay, and packet overhead in comparison with other mobility schemes.

The remaining of this paper is organized as follows. First of all, we make a brief survey of related works of micro-mobility management in network mobility. The overview of Micro-NEMO, the associated handoff mechanism, and enhanced scheme for resolving pinball routing problem are explained in section 3. Simulation environment and results for performance evaluation are presented in section 4. Finally, section 5 concludes this paper.

2 Related Work

Generally, there are two types of micro-mobility issues in discussion of network mobility: (1) extra-NEMO micro-mobility [9-12] and (2) intra-NEMO micro-mobility [13, 14]. The extra-NEMO micro-mobility means that mobile network moves around the micro-domains, which is similar to host micro-mobility. The intra-NEMO micro-mobility is the mobility management for the internal vehicle, i.e., a single transportation is regarded as a micro-domain. Since the focus of this work is on extra-NEMO micro-mobility, we do a literature survey on recent research works on extra-NEMO works in the following.

A micro-mobility scheme in [9] developed by Ohnishi, which is called Ohnishi scheme in this paper, is aimed to solve the pinball routing problem in network mobility rather than to provide a micro-mobility scheme for a moving network. Here, we first briefly discuss some famous issues of micro-mobility of host mobility - HMIPv6 [3]. In HMIPv6, mobile host moving within micro-domain performs local binding update with mobile anchor point (MAP) rather than home registration. The Ohnishi scheme is extension of HMIPv6. In Ohnishi scheme, each VMN still performs binding update by itself even when VMN gets on the vehicle. Thus, the Ohnishi scheme does not include the concept of network mobility. Therefore, even Ohnishi scheme can be backward compatible with HMIPv6 and several works about micro-mobility of network mobility issue have been proposed based on Ohnishi such as [10], we still believe that Ohnishi scheme is inappropriate for network mobility and use it as one of the compared schemes in performance evaluation section.

Besides, some works such as [11, 12] are about extra-NEMO micro-mobility. In [11], authors proposed a route optimization methodology that uses unidirectional

tunneling and a tree-based intra-domain routing mechanism and declare that it can be easily extended to support micro-mobility. However, it could not be backward compatible with conventional host micro-mobility. So that mobile host may not perform micro-mobility when it gets off the vehicle. Another work in [12] proposed the HMIP-B (Hierarchical Mobile IPv6 extension with buffering function) scheme, in which MAP store packets destined to the mobile hosts during the process of handoff. That is, the focus of HMIP-B is to reduce packet loss rather than to provide a micro-mobility scheme.

3 Micro-mobility Scheme for Mobile Network

3.1 Protocol Overview

Micro-NEMO, as depicted in Figure 1, is aimed to support simultaneous (multiple consequent) local movements within an administrative domain (micro-domain) for a mobile network. Hence, the major idea of Micro-NEMO scheme is to include the concept of micro-mobility into NEMO protocol while preserving both the characteristics of micro-mobility and NEMO protocols. That is, Micro-NEMO is designed to achieve low handoff latency, has minimal signaling cost and be transparent to all the mobile hosts within the same mobile network, i.e., mobile hosts inside that moving network will not perceive that the MR has changed point of attachment. At last, to be compatible with the NEMO basic support protocol that is extended by MIPv6 as HMIPv6, Micro-NEMO is built from HMIPv6 as well.

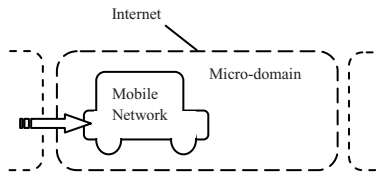


Fig. 1. Micro-mobility Scheme for mobile network

3.2 Local Movement Scenarios for Mobile Network

To design the Micro-NEMO, we begin with understanding the relationship between VMN and transportations. In general, there are four movement scenarios for micro-mobility of mobile network as shown in Figure 2. First, the location management happens when mobile network initially enters a new micro-domain as illustrated in Figure 2(a). This is similar to that a mobile host first gets into a new micro-domain. Second, a visit mobile node (VMN), which is like that a human has a mobile device such as mobile phone, gets on the transportation as illustrated in Figure 2(b). Next, Figure 2(c) depicts that the mobile network roams within a micro-domain. Finally, the case in Figure 2(d) is that VMN takes off the transportation.

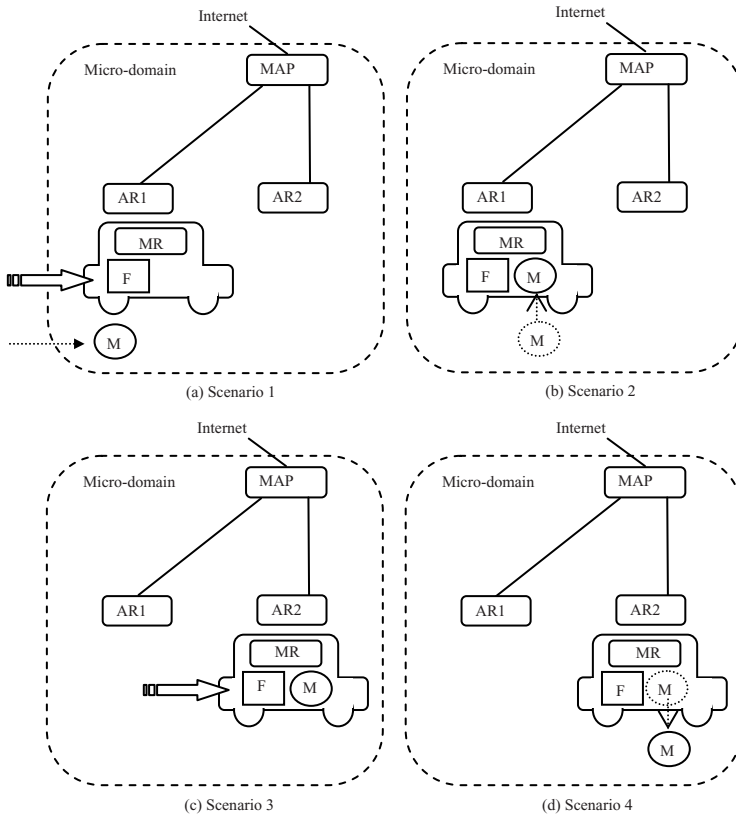


Fig. 2. Scenarios for Micro-NEMO

3.3 Protocol Description

As discussed before, there are four types of scenarios for mobile network in the micro-domain environments. In this section, we describe all the details of operations for each scenario in the following.

Scenario 1. When a vehicle (mobile network) enters a new micro-domain, the MR of that vehicle starts to perform the operation of micro-mobility scheme to allow the home agent of MR can be aware of the location of the vehicle. Figure 3 (a) and (b) shows that the signaling flow and the data delivery respectively for a vehicle entering the micro-domain at the first time. The MR of the vehicle will obtain the on-link care-of-address (LCoA) and regional care-of-address (RoA), and it registers with MAP to establish a binding. Then, MR performs home registration with HA of MR. After these initial signalings are finished, that home network (home link) of the vehicle knows on which micro-domain the vehicle is. Once a CN wants to transmit data packet to LFN (local fixed node), the data packets pass through HA of MR, MAP and reach LMN finally.

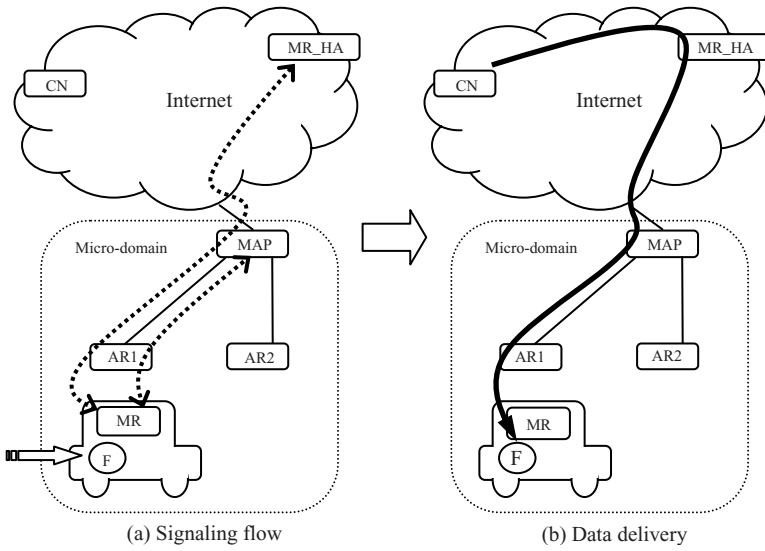


Fig. 3. When a vehicle (mobile network) first enter a micro-domain

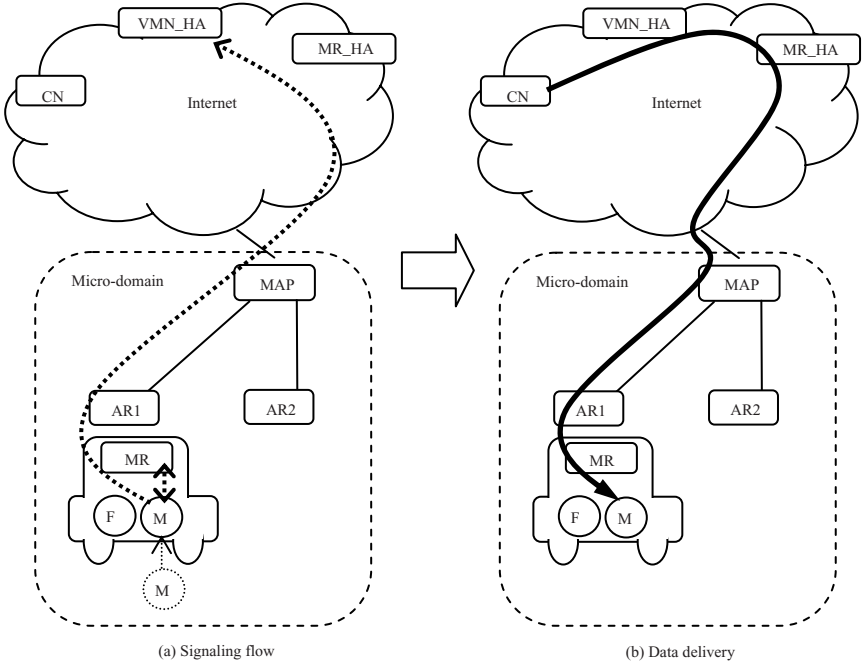


Fig. 4. When a VMN get on the vehicle

Scenario 2. Figure 4 shows that a VMN gets on a vehicle within a micro-domain. In this case that VMN will inform its home agent (HA) once and the mobile router (MR) of the mobile network will perform location management function on behalf of VMN(s) as the vehicle movement. After VMN obtains a CoA from MR, it starts to perform home registration once as illustrated in Figure 4(a). Afterward there is no need home registration between VMN and its HA. As for the data delivery, data packets sent by CN will be tunneled by the HA of VMN and the HA of MR respectively, then pass through MAP and arrive at VMN finally as illustrated in Figure 4(b).

Scenario 3. Based on the concept of the micro-mobility, there is no need for MR of a vehicle to perform home registration when it moves around within the same micro-domain. In other words, it only needs to obtain a new LCoA and perform local binding update to the MAP in order to establish a binding between the LCoA and RCoA. In addition, all VMNs within that vehicle do not carry out any binding updates except the home registration at the first time.

Scenario 4. Lastly, when a VMN gets off the vehicle, this case is similar to that a VMN enters a new micro-domain. Since the VMN is not in a mobile network any more and should perform micro-mobility scheme by itself, VMN starts to do the process of host mobility.

3.4 Advantage and Drawback

In order to provide an efficient scheme integrating both micro-mobility and network mobility, we proposed a Micro-NEMO protocol. In this basic solution, we directly apply micro-mobility concept into the Micro-NEMO protocol, i.e., a vehicle only needs to perform local binding update with MAP when it moves within an administrative micro-domain. Specifically, the mobile network does not perform home registration with HA unless it traverses to a new micro-domain. As a consequence, the number of global binding updates could be reduced. On the other hand, Micro-NEMO protocol is corresponding to the concept of network mobility as well, i.e. the mobility of the vehicle is transparent to its residing nodes (e.g. local fixed nodes and visiting mobile nodes). However, we note that Micro-NEMO still suffers from the same drawback, i.e., the pinball routing problem in Figure 4(b), as the basic NEMO protocol does. That is, data packets will be tunneled through multiple HAs (both HAs of VMNs and HA of MR) before it arrives to the destination host. This not only results in sub-optimal end-to-end path, but also incurs heavy packet overheads. Moreover, the problem becomes more critical if the number of levels of nested NEMO increases. Next, we will propose an enhanced Micro-NEMO protocol to deal with the pinball routing problem.

3.5 Enhanced Approach

We note that the pinball routing problem can be solved if the HA of the root MR knows all the binding information of child MRs and VMNs. Hence, the HA of the root MR is able to perform binding update with the sender (CN) by RCoA of root MR. Afterward, CN could directly forward packets to VMN of the vehicle inside a micro-domain.

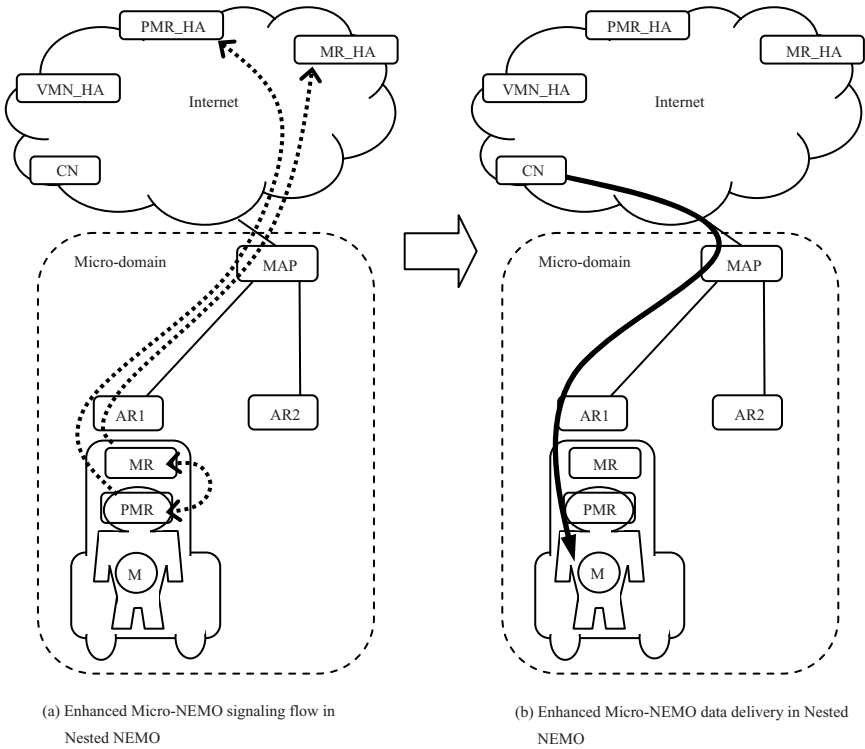


Fig. 5. Enhanced Micro-NEMO Protocol

Figure 5 shows that signaling flow and data delivery of enhanced Micro-NEMO. When a human with a personal area network (PAN) gets on a vehicle, MR needs to inform HA of MR of location information of nodes inside entering moving network and PMR (MR of PAN) also has to perform home registration with its HA as illustrated in Figure 5(a). Once HA of MR receives packet sent from HA of child node, it could perform binding update with CN. Afterward CN is able to directly forward data packets through MAP to the VMN as depicted in Figure 5(b). Hence, our enhanced approach could efficiently cope with the pinball routing problem. That is, the enhanced approach could not only shorten end to end delay between sender CN and VMN for nested NEMO but also reduce packet overheads through getting rid of multiple tunneling.

4 Performance Evaluation

4.1 Simulation Environment and Performance Criteria

Simulation study has been conducted to evaluate the performance of Micro-NEMO as well as the enhanced approach. There are total 64 micro-domains in the simulation,

i.e., an 8×8 mesh grids. Each micro-domain mesh grid is equipped with a MAP. Moreover, each MAP contains 16 ARs, in 4×4 sub-grids and each sub-grid has an AR. There are total 500 moving vehicles randomly scattered over all micro-domains. Each vehicle has a MR and 5 VMNs and the total number of VMN is 2500. In order to model the mobility of the vehicle, time is slotted and *MoveProb*(Movement Probability) is used in the simulation. *MoveProb* represents the probability of a vehicle leaves its current AR in the next time slot. When a vehicle decides to leave the current AR in the next time slot, its next AR is randomly selected from the neighboring ARs. Details of the simulation parameter are described in Table 2.

Table 2. Simulation parameters

| | |
|--|---|
| MR(Vehicle)# = 500 VMN# = 2500, 5 VMNs per MR MoveProb (Movement Probability) = 0.8 Simulation Time = 1000 time units | |
| Delay latency | Internet latency = 50 time units Local domain latency = 10 time units Backbone latency = 1 time units |

Four performance metrics are used to compare the proposed Micro-NEMO basic and enhanced scheme with other schemes and they are: (1) total number of binding updates, (2) the average handoff latency, (3) end to end delay, and (4) packet overhead. The average handoff latency is defined as the time to complete binding update after a handoff, the end to end delay is defined as the time interval for a data packet from sender to receiver, and the packet overhead is defined as the ratio of encapsulate packet headers size to total packet size.

4.2 Simulation Results

Figure 6 shows the total number of binding update under different schemes. To compare with basic NEMO protocol, the number of global binding update of Micro-NEMO is lower than basic NEMO protocol since it could effectively integrate the idea of the micro-mobility. In addition, the total number of binding updates in both HMIP and Ohnishi scheme is higher than Micro-NEMO because they do not consider the concept of network mobility, i.e., they ignore the characteristic of the mobile network, all the mobiles hosts within the same mobile network can update their location information through a “*single*” binding update of MR of that mobile network. In other words, when the MR changes its access point, all mobile hosts inside the moving network will not observe that change such that the binding update storm for all MHs can be avoided.

Comparison of the average handoff latency is depicted in Figure 7. Since the proposed scheme can provide the functionality of micro-mobility, it is not surprising that the latency is lower than NEMO, HMIP and Ohnishi. Next, Figure 8 shows that the results of the end to end delay for different schemes. Since the proposed enhanced Micro-NEMO scheme is equipped with the process of route optimization, the end to

end delay has been significantly decreased. At last, due to the same reason, i.e., the route optimization functionality, Figure 9 also shows that enhanced Micro-NEMO is much better than other schemes in terms of packet overhead.

Please note that we have performed a wide range of simulations for different parameter settings, e.g., *MoveProb* values, mobility pattern and vehicle speed etc. Due to the limit space of the paper, we only use the case of *MoveProb* = 0.8 in the paper. Qualitatively, the similar trend still persists.

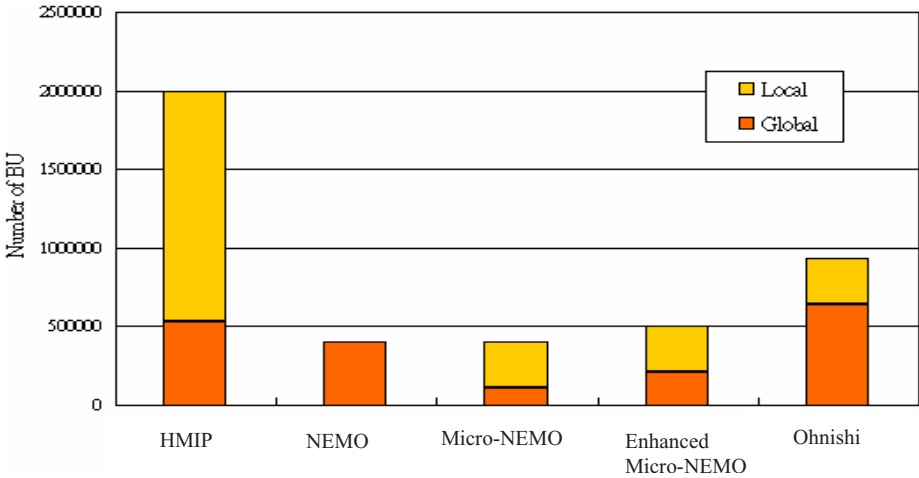


Fig. 6. Total number of binding update

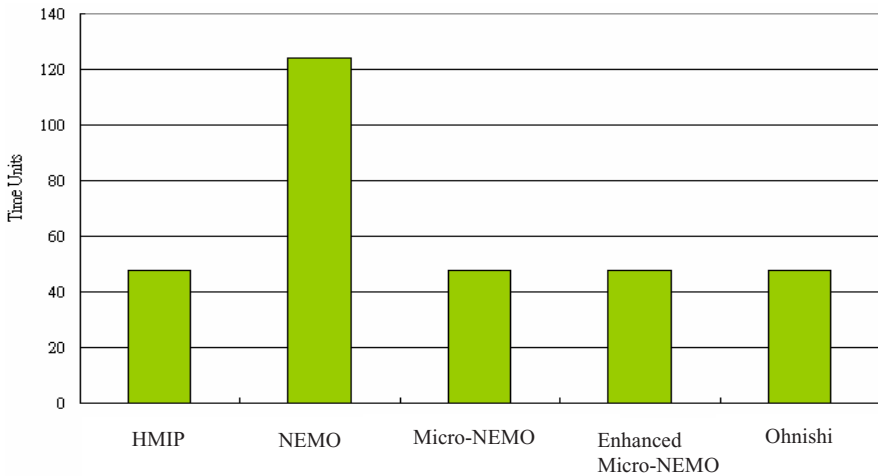


Fig. 7. Average handoff latency

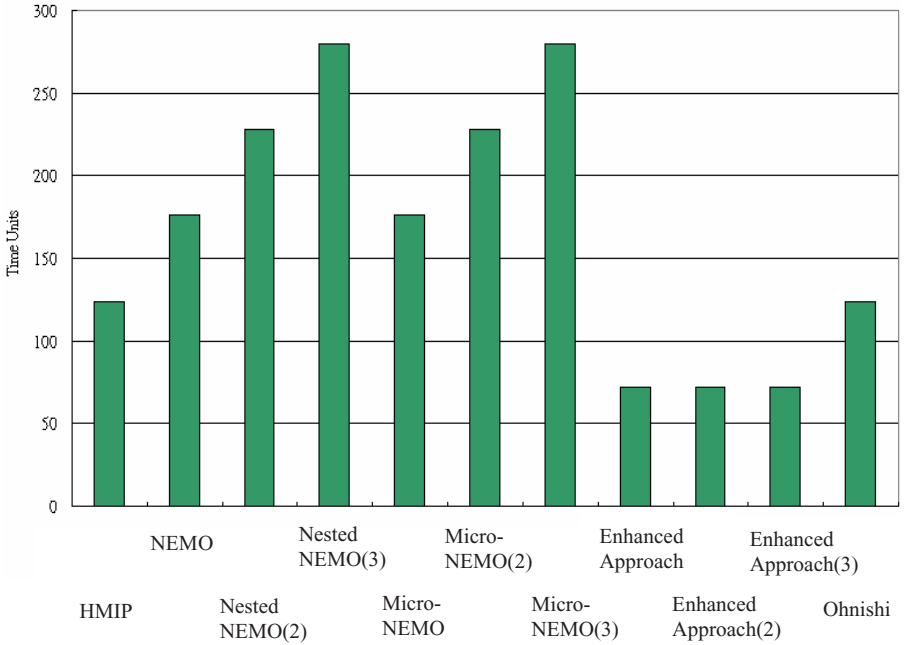


Fig. 8. End to end delay

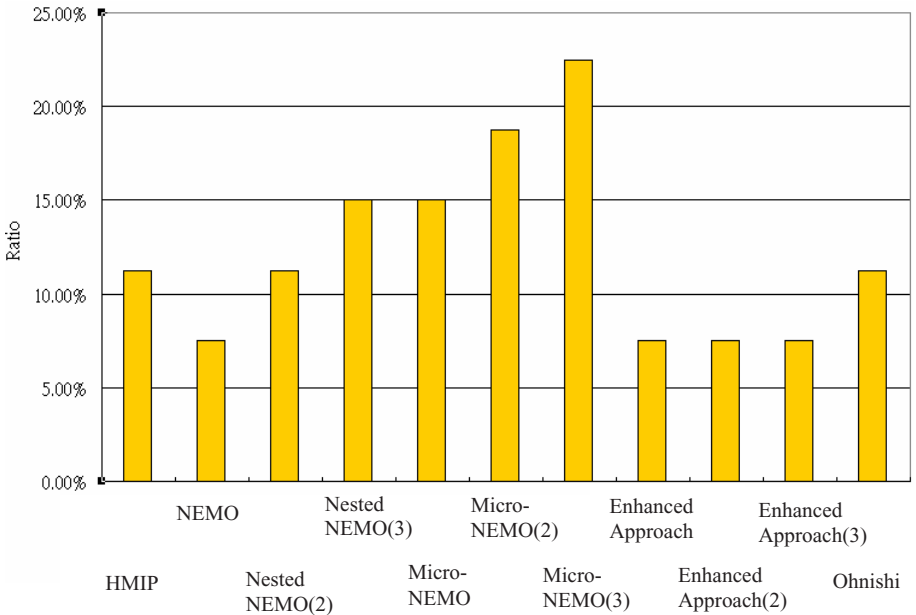


Fig. 9. Packet Overhead

5 Conclusion

In the past decade, there are plenty of research works focusing on micro-mobility issue for the host mobility protocol. Since the network mobility has attracted much attention recently, we believe there is a need to support the functionality of micro-mobility for NEMO. In this paper, we propose a micro-mobility scheme for mobile network (Micro-NEMO). To be backward compatible with NEMO, the proposed scheme is extended from HMIPv6. The scheme can provide local movement of vehicle and integrate to micro-mobility of the single mobile host. Furthermore, to deal with the pinball routing problem, we provide an enhanced Micro-NEMO, which is able to perform the procedure of route optimization. Simulation results have showed that Micro-NEMO and enhanced scheme are able to improve the number of binding update, average handoff latency, end to end delay, and packet overhead in comparison with other mobility schemes.

References

1. Johnson, D., Perkins, C., Arkko, J.: IP Mobility Support. IETF, RFC 2002 (1996)
2. Perkins, C.: Mobile IP. *IEEE Communication Magazine* 35(5), 84–99 (1997)
3. Soliman, H., Castelluccia, C., El Malki, K., Bellier, L.: Hierarchical Mobile IPv6 Mobility Management (HMIPv6). IETF, RFC 4140 (2005)
4. Campbell, A., Gomez, J., Kim, S., Valko, A., Wan, C., Turanyi, Z.: Design implementation and evaluation of cellular IP. *IEEE Personal Communications* 7(4), 42–49 (2000)
5. Campbell, A., Gomez, J., Kim, S.: An Overview of Cellular IP. In: WCNC. Proceeding of IEEE Wireless Communications and Networking Conference, vol. 2, pp. 606–610 (1999)
6. Ramjee, R., Varadhan, K., Salgarelli, L., Thuel, S., Wang, S., Porta, T.L.: HAWAII: A domain-based approach for supporting mobility in wide-area wireless networks. *IEEE/ACM Transactions on Networking* 10(3), 396–410 (2002)
7. Lach, H.-Y., Janneteau, C., Petrescu, A.: Network mobility in beyond-3G systems. *IEEE Communication Magazine* 41(7), 52–57 (2003)
8. Devarapalli, V., Wakikawa, R., Prtrescu, A., Thubert, P.: Network Mobility (NEMO) Basic Support Protocol. IETF, RFC 3963 (2005)
9. Ohnishi, H., Sakitani, K., Takagi, Y.: HMIP based route optimization method in a mobile network. IETF, Internet Draft (2003)
10. Novak, R.: Proxy MAP for Intra-domain Route Optimization in Hierarchical Mobile IP. *IEICE Transactions on Communications* E89-B(2) (2006)
11. Jeong, M.-S., Park, J.-T.: Hierarchical Mobile Network Routing: Route Optimization and Micro-Mobility Support for NEMO. In: Yang, L.T., Guo, M., Gao, G.R., Jha, N.K. (eds.) *EUC 2004*. LNCS, vol. 3207, pp. 571–580. Springer, Heidelberg (2004)
12. Omae, K., Inouem, M., Okajima, I., Umeda, N.: Handoff performance of mobile host and mobile router employing HMIP extension. In: WCNC. Proceeding of IEEE Wireless Communications and Networking Conference, vol. 2, pp. 1218–1222 (2003)
13. Rónai, M.A., Fodor, K., Tönjes, R.: IPv6 Moving Network Testbed with Micro-Mobility Support. *IST Mobile and Wireless Communications*, 596–600 (summit, 2004)
14. Watanabe, Y.: A Micro Mobility Protocol for Network Mobility with Fast Handovers. In: *The International Conference on Internet Networking* (2006)

ANSWER: Adaptive Network Selection in WLAN/UMTS EnviRonment*

Chih-Cheng Hsu¹, Ming-Hung Chen¹, Cheng-Fu Chou¹,
Wei-Chieh Chi¹, and Chung-Yi Lai²

¹ Dept. of Computer Science and Information Engineering,
National Taiwan University, Taipei, Taiwan, R.O.C.
{Kenneth, mhchen, ccf, hypec}@cmlab.csie.ntu.edu.tw

² Institute for Information Industry, Taiwan, R.O.C.
laici@iii.org.tw

Abstract. The next generation wireless network is aimed to provide users with anywhere, anytime, and seamless service. With the increasing demand for the next generation network, many research works have focused on the efficient way to integrate different types of heterogeneous wireless networks such as cellular systems and wireless LAN. Therefore, the network selection technique plays a critical role in ensuring quality of service for the next generation network. In this paper, we propose an adaptive network selection (ANSWER) scheme, which is able to make the better decision about when to switch and choice on which access network. That is, we want to provide the always-best-connected service as much as possible for the users. Specifically, to achieve the above goals, the available bandwidths of all possible networks, the location of user's device and its moving direction are taken into consideration in the ANSWER approach. We evaluate the performance of the ANSWER scheme through extensive simulations and the results agree with our goals.

Keywords: seamless, heterogeneous wireless network, available bandwidth, network selection.

1 Introduction

With the increasing demand for high data rate multimedia services, commercial third-generation (3G) cellular network and handsets are gradually rolling into the market. Compared to cellular networks, WLAN (IEEE 802.11b offers a data rate up to 11Mb/s) is able to offer higher transmission bandwidth at a lower cost but cover smaller geographic areas. As a result, the WLAN is regarded as a proper candidate for high data rate services at certain hotspot areas with low user's mobility.

* This work was partially supported by the National Science Council and the Ministry of Education of R.O.C. under the contract No. NSC95-2221-E-002-103-MY2 and NSC95-2622-E-002-018.

To provide anywhere, anytime, and seamless service, the next generation wireless network is expected to be a heterogeneous network, which can efficiently integrate several different characteristic access networks. Mobile users may move among these heterogeneous networks by seamlessly switching between different serving stations. How to take advantage of the wide coverage support of cellular network and the high data rates of WLANs is a challenge.

In cellular network, resource allocation is implemented by properly scheduling access to wireless channel to provide QoS guarantee. However, there is no user QoS guarantee in the current IEEE 802.11 WLAN standard. The latest IEEE 802.11e standard only enhances relative QoS. Besides, different traffic types usually require different QoS deliveries. Real-time services such as voice and video are sensitive to end-to-end delay, while the main concern of delay-tolerant data service is throughput. WLANs are more efficient than cellular networks in serving bursty data traffic, while it is quite difficult for WLANs to meet the strict delay requirements. Hence, the differences of QoS support in these two networks need to be considered for resource management.

While the moving speed of a mobile device is higher, more handoffs may occur during the lifetime of a call. The handoff procedure would cause extra delay, e.g., packet losses or even connection interruption. Moreover, handoff traffic should be separated from new traffic in terms of call admission. Thus, network selection algorithms and admission control for different requests are investigated.

In this work, we focus on finding the better access network between IEEE 802.11 WLAN and UMTS (Universal Mobile Telecommunications System) for the user device with two types of interfaces. Although the capacity of WLAN is larger than that of UMTS, the current available bandwidth of WLAN may decrease to be lower than the bandwidth guaranteed in UMTS when a lot of users stay in WLAN. In our proposed approach, we estimate the current available bandwidth of WLAN and the user dwell time in WLAN; then we make a handoff decision based on the information gathered. Since the coverage of UMTS network is much wider than that of WLAN, we assume that UMTS service always exists. Our contributions are estimating the network condition, predicting user's moving behavior and deciding if it is beneficial to make vertical handoff.

The remainder of the work is organized as follows. In section 2, we discuss related work about the UMTS-WLAN internetworking. In section 3, we describe the overall network selection algorithm including the basic idea, assumption, and detail procedures. In section 4, we evaluate the performance of proposed approach. Finally, we conclude the paper and give future works in section 5.

2 Related Work

In traditional selection methods such as [1], only radio signal strength (RSS) threshold and hysteresis values are considered. However, they do not take the current condition or user's preference into account. When more handoff decision factors are considered, two-dimension cost functions, such as [2], are proposed. In one dimension, the function reflects the types of service (ToS) requested by the user, and another dimension represents the cost to network according to specific parameters. The paper

in [3] separates cost function factors into different categories: QoS factors, weighting factors, and network priority factors. QoS factors are defined based on user-specific requirements. The weight factors stand for the importance of the particular requirements with respect to the user. The network priority factors present the abilities of the networks to meet the requirements.

In [4], analytic hierarchy process (AHP) and the grey relational analysis (GRA) are integrated into the network selection algorithms. AHP is used to derive the weights of the parameters based on user's preference and service application. GRA takes charge of ranking the network alternatives. Some research works in [5] and [6] use dwell-timer to alleviate frequent handoffs and improve performance in transition area. They also investigate the effect of dwell-timer as the throughput ratio of WLAN and UMTS is changing. In [7], location information is shown to be beneficial to the accuracy of handoff decision in multi-service networks.

[8] [9] show that although the WLAN QoS capabilities have been extended with the introduction of IEEE 802.11e, the WLAN is still unable to support all QoS features provided by UMTS. Without affecting the service provided to existing WLAN data users, there is a limited number of UMTS roamers to be accepted in the WLAN depending on the bandwidth reservation and QoS requirements.

[10] presents a framework for a service provider to perform resource management in heterogeneous wireless networks. The proposed architecture allows the service provider to support real-time resource management functions based on Service Level Agreement (SLA) and seamless service handoff.

The experimental measurements of VoIP on 3G-WLAN internetworking system in [11] show that in addition to the VoIP connections, the performance of all clients in WLAN can degrade significantly due to the unfairness, undistinguished real-time and non real-time traffic of the packet queue in the AP and the inherent property of IEEE 802.11. In [12], they focus on the wireless multimedia distribution applications and recognize that service continuity is an important quality requirement. It designs and implements this class of applications on top of a session layer providing download continuity support when user changes location, network or terminal.

3 ANSWER Framework

In most of previous research works, the bandwidth in the WLAN is assumed to be greater than that in UMTS. However, for wireless networks, some conditions such as medium contention, channel fading, and interference, influence the available bandwidth. Furthermore, at the boundary of the WLAN cell, the received signal strength (RSS) varies around some thresholds. Such situation might cause frequently sequential vertical handoffs. This is not desired because the handoff procedure always demands extra time and no data traffic can be carried to or from mobile users during the procedure.

Therefore, instead of always switching to WLAN, evaluating the benefit of making vertical handoff is the main concern. The basic concept of our approach is: estimating the current available bandwidth of WLAN and predicting moving direction of mobile users to avoid unnecessary handoff.

Assumptions

- Mobile IP allows users in an environment with two wireless networks.
- Mobile host is aware of its current position, speed, and direction by GPS.
- Coordinates of AP can be broadcast.
- UMTS network is always achievable and guarantee a certain amount of bandwidth.

Table 1. The definition of notations used in this work

| Variable | Description |
|---------------|--|
| BW_{WLAN} | Available bandwidth in WLAN |
| BW_{UMTS} | Available bandwidth in UMTS |
| P_r | Receiving power of access point |
| $RXTresh$ | Receiving threshold in WLAN |
| Δ | Vertical handoff delay |
| T | Sojourn time of the mobile host in WLAN cell |
| \mathcal{V} | Velocity of mobile host |
| R | Transmission range of WLAN |

Table 1 gives the definition of notations used in this work, BW_{WLAN} is assessed by using the approach described in section 3.1. BW_{UMTS} is a constant value since we assume that certain bandwidth is reserved for the mobile host. P_r is measured from the packets sent from the base station. $RXTresh$ is the minimal necessary power level for a packet to be successfully received. Δ comes from the vertical handoff procedure as the mobile host switches between different access networks. In section 3.2, we will introduce how we measure the value of T . \mathcal{V} is the current speed of the mobile host.

3.1 Available Bandwidth Estimation

The bandwidth estimation approach in [13] [14] is adopted in this article. Figure 1 shows the packet transmission sequence in IEEE 802.11. They measure the throughput TP of transmitting a packet as $TP = S / (t_r - t_s)$, where S is the size of the packet, t_s is the time-stamp that the packet is ready at the MAC layer, and t_r is the time-stamp that an ACK has been received. The time interval $t_r - t_s$ includes the channel busy and contention time. It is clear that the measured throughput of a packet depends on the size of the packet. A larger packet has higher measured throughput because it sends more data once it grabs the channel. To make the throughput

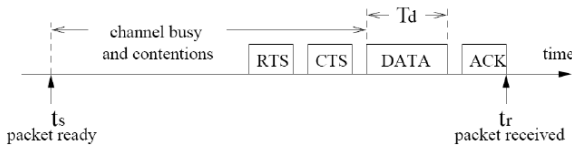


Fig. 1. IEEE 802.11 unicast packet transmission sequence

measurement independent of the packet size, they normalize the throughput of a packet to a pre-defined packet size.

In Figure 1, $T_d = S / BW_{ch}$ is the actual time for the channel to transmit the data packet, where BW_{ch} is the channel's bit-rate. Here they assume channel's bit-rate is a pre-defined physical layer parameter. The transmission times of any two packets should differ only in their times to transmit the DATA packets. Therefore, the following equation holds:

$$(t_{r1} - t_{s1}) - \frac{S_1}{BW_{ch}} = (t_{r2} - t_{s2}) - \frac{S_2}{BW_{ch}} \quad (1)$$

$$\Rightarrow (t_{r1} - t_{s1}) - \frac{S_1}{BW_{ch}} = \frac{S_2}{TP_2} - \frac{S_2}{BW_{ch}} \quad (2)$$

Where S_1 is the actual data packet size and S_2 is a pre-defined standard packet size. We can use Equation (2) to calculate normalized throughput TP_2 for the standard size packet and use the normalized throughput to represent the available bandwidth of wireless link.

3.2 Sojourn Time Estimation

We predict MH's sojourn time in WLAN by its current speed and its distance to the edge of WLAN cell. In the hotspot, MH simply moves with some velocity from one waypoint to another. As illustrated in Figure 2, the solid line represents the actual moving path of the MH, and the dotted line stands for the path we predict the MH will move along. Since we know the moving direction of MH and the coordinates of both MH and AP, two vectors, \vec{a} and \vec{b} , are obtained. By the definition of inner product:

$$\vec{a} \cdot \vec{b} = |\vec{a}| |\vec{b}| \cos \theta, \quad (3)$$

where θ is the angle between \vec{a} and \vec{b} , $\cos \theta$ is derived. Then based on the cosine rule:

$$R^2 = |\vec{b}|^2 + L^2 - 2L|\vec{b}|\cos \theta \quad (4)$$

The distance to the edge of WLAN cell, namely L , is obtained by equation (4). Therefore, the dwell time in WLAN is $T = L / v$, and even if MH is not in the AP coverage, T represents the time to meet the boundary of WLAN.

3.3 Network Selection Algorithm

With the information gathered in 3.1 and 3.2, we describe the network selection procedure in Algorithm 1. Normally, the procedure should be executed for each probing interval t . However, in order to reduce overhead caused by frequently probing, we introduce a sleep time t into the algorithm (Step 5 and 21). Step 1 to 5 gather the necessary information and stay in UMTS if no WLAN service is available. Once MH enters the AP coverage, the handoff decision is made based on the value *cost*.

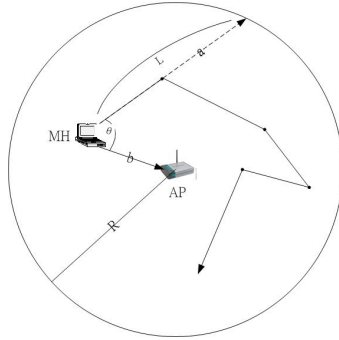


Fig. 2. Moving behavior of a mobile host

The idea of *cost* is: Is making handoff profitable for the throughput in next t seconds? If MH is currently connected to UMTS and continues using UMTS service, no handoff is needed when MH leaves the WLAN. On the contrary, if MH switches to WLAN, two handoffs are made when MH switches back to UMTS. Similarly, if MH is currently connected to WLAN, only one handoff is made throughout the procedure no matter MH switches to UMTS or not. Thus, different situations result in different objective functions (Step 11 and 13). Note that we add α in the objective function to reduce oscillation. We prefer to stay in UMTS network when the bandwidth of WLAN approximates that of UMTS because WLAN network no longer has high bandwidth, which is its main advantage over UMTS network.

Algorithm 1 Network Selection Procedure

```

1: Send probing packets
2: Estimate  $BW_{WLAN}, P_r, v, T$ 
3: if  $P_r < RXThresh$  then
4:   Stay in UMTS
5:   Go to sleep for  $t$  sec
6: else
7:   if  $v == 0$  then
8:      $cost \leftarrow (BW_{WLAN} + \alpha) - BW_{UMTS}$ 
9:   else
10:    if MH is connecting to UMTS network then
11:       $cost \leftarrow (BW_{UMTS} + \alpha) * T - BW_{WLAN} * (T - 2 * \Delta)$ 
12:    else
13:       $cost \leftarrow (BW_{UMTS} + \alpha) * (T - \Delta) - BW_{WLAN} * (T - \Delta)$ 
14:    end if
15:  end if
16:  if  $cost > 0$  then
17:    Stay in or make handoff to UMTS network
18:  else
19:    Stay in or make handoff to WLAN network
20:  end if
21:  If any handoff is made, go to sleep for  $t$  sec
22: end if

```

4 Performance Evaluation

We will show and discuss the performance of our approach compared with the WLAN-first and UMTS-first approach. Section 4.1 describes our simulation environment and performance metrics.

4.1 Network Environment and Performance Metrics

To conduct our experiment, we use the NS-2 (Network Simulator 2) with the UMTS extension from [15]. We set up our WLAN-UMTS networks according to the parameters exposed in Table 2. Total simulation time is 500 seconds, and as to the data traffic destined to MH, performances of CBR/UDP traffic are assessed respectively. Two metrics are used for our performance evaluation:

- Goodput: (total bits received - retransmitted bits) / measurement interval
- Number of handoffs: The quantity of handoffs MH made in its lifetime.

Table 2. Parameters used in performance evaluation

| Parameter | Value |
|--|-------------|
| Topology | 1000m×1000m |
| WLAN Capacity | 11 Mbps |
| UMTS Capacity | 384 Kbps |
| RXThresh | 3.6526e-10 |
| Vertical handoff delay | 0.1 sec |
| Number of Poisson background traffic in WLAN | 10 to 60 |
| Packet size of Poisson traffic | 1000 byte |
| Average data rate of a Poisson traffic | 100 Kbps |
| Probing packet size | 64 byte |

4.2 Mobility Model

Three most popular mobility models are used in our simulation, and the brief descriptions are the following:

- ◆ **Random Waypoint Model:** the Random Waypoint model is the most commonly used mobility model in research community. In the current NS-2, the implementation of this mobility model is as follows: at every instant, a node randomly chooses a destination and moves towards it with a velocity chosen uniformly randomly from $[0, V_{max}]$, where V_{max} is the maximum allowable velocity for every mobile node. When reaching the destination, the node stops for duration. After this pause time, it again chooses a random destination and repeats the whole process again until the simulation ends.
- ◆ **Freeway Mobility Model:** this model emulates the motion behavior of mobile nodes on a freeway. Maps are used in this model. There are several freeways on the map and each freeway has lanes in both directions. The differences between Random Waypoint and Freeway are the following: (1) Each mobile node is restricted to its lane. (2) The velocity of mobile node is dependent on its previous velocity. (3) If two mobile nodes on the same freeway lane are within the safety distance, the velocity of the following node cannot exceed the velocity of preceding node. It also imposes strict geographic restrictions on the node movement by not allowing a node to change its lane.

- ◆ **Manhattan Mobility Model:** Manhattan model emulates the movement pattern of mobile nodes on streets defined by maps. It can be useful in modeling movement in an urban area. The map of the Manhattan model is composed of a number of horizontal and vertical streets. The mobile node is allowed to move along the grid of horizontal and vertical streets on the map. At an intersection of a horizontal and a vertical street, the mobile node can turn left, right or go straight with certain probability. Except the above difference, the node relationships involved in the model are very similar to the Freeway model. However, it differs from the Freeway model in giving a node some freedom to change its direction.

The maximum speed and pause time in random waypoint model are 10 m/s and 10 seconds respectively in our simulation. The speed in Freeway mobility model ranges from 10 to 60 m/s, and the maximum speed in Manhattan model is 10 m/s.

4.3 Goodput Comparison

From Figure 3 (a) to (c), we can see that our approach ANSWER greatly outperforms WLAN-first and UMTS-first method in CBR traffic, no matter network load in WLAN is heavy or not. Our approach will mostly stay in UMTS network when the WLAN is too crowded (number of background traffic is 30 to 50) and efficiently utilize the high bandwidth of WLAN when network load of WLAN is light (number

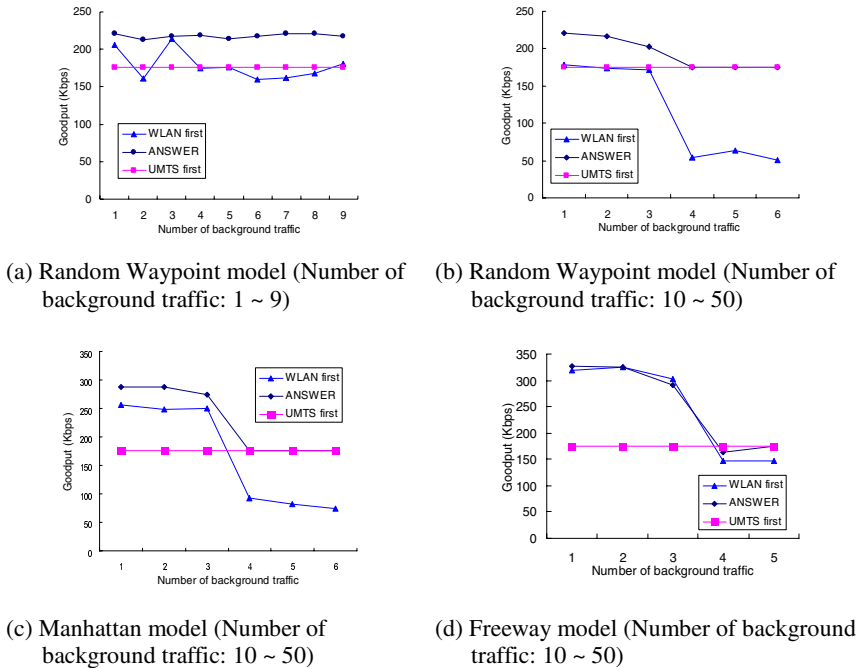
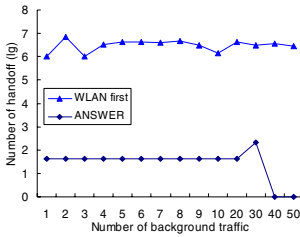


Fig. 3. CBR goodput comparison in different mobility model

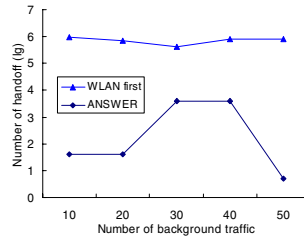
of background traffic is 10 to 30). In Figure 3(d), the performance of freeway mobility model is not good as that in the other two mobility model when the background traffic in WLAN increases, because MH rushes in and out as its moving speed is fast.

4.4 Number of Vertical Handoffs

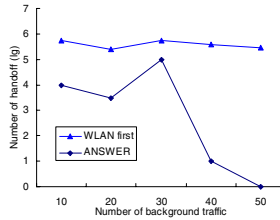
Vertical handoff causes call intermission, so in this section we focus on how many handoffs MH makes throughout the whole course. Figure 4 show that number of handoff in our approach is much less than that in WLAN-first method. Our selection algorithm efficiently reduces many unnecessary handoffs by predicting MH's sojourn time.



(a) Number of handoff in Random Waypoint model



(b) Number of handoff in Manhattan model



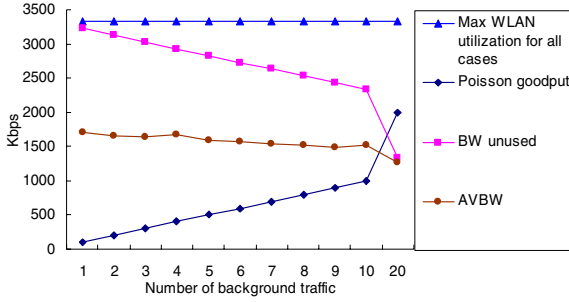
(c) Number of handoff in Freeway model

Fig. 4. Number of handoff in different mobility model

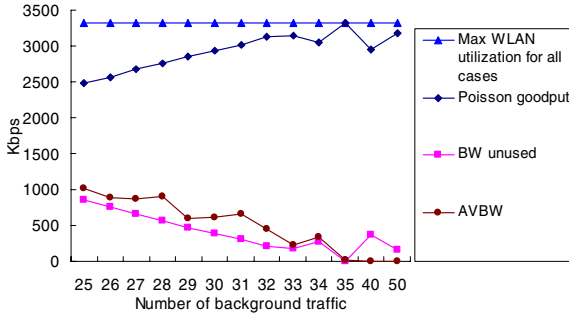
4.5 Accuracy of Available Bandwidth

To measure the accuracy of the estimated available bandwidth, we first assume the total usable bandwidth in WLAN to be the maximum WLAN utilization achieved in our simulations, which is about 3Mbps. Thus, the bandwidth unused by the Poisson background traffic is the approximation of actual available bandwidth. The comparison of the approximation and the estimated value by the approach in section 3.1 is in Figure 5.

When the network load is light, the bandwidth estimated is about 1700 Kbps at most. The reason is that $t_r - t_s$ in Figure 5(a) has a minimum value since the



(a) Comparison when Number of background traffic: 1 to 20



(b) Comparison when Number of background traffic: 21 to 50

Fig. 5. Comparison between estimated and actual bandwidth

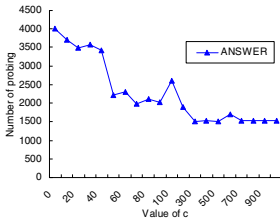
contention period in IEEE 802.11 can not be reduced unlimitedly. When the load increases, the two curves become closer to each other. Although the estimated value is not highly precise, the two curves go in the same trend.

4.6 Dynamic Sleep Time

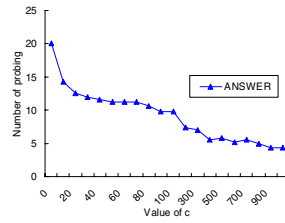
We adjust the sleep time t in our algorithm based on speed and available bandwidth on the instant, as equation (5) shows.

$$t = c \times \frac{BW_{WLAN}}{BW_{UMTS}} \times \frac{1}{v} \tag{5}$$

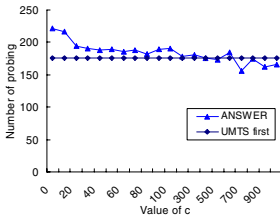
CBR traffic destined to MH in Random Waypoint model is simulated and the number of background traffic is set to 30. We can see that there is a tradeoff between goodput/jitter and number of handoff/probe in Figure 6. As c increases, MH would miss some opportunities to switch to the better network in sleep time but it would send fewer probing packets.



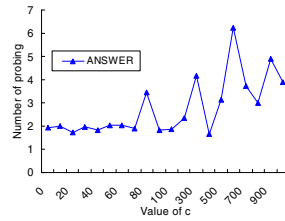
(a) Number of probe



(b) Number of handoff



(c) Goodput



(d) Average jitter

Fig. 6. Simulation results for different value of c

5 Conclusion and Future Works

In this work, we have proposed an approach dealing with network selection from WLAN and UMTS network. The approach estimates current available bandwidth and sojourn time in WLAN to choose the better network. The simulation in this paper shows that our algorithm achieves better performance and has fewer handoffs than UMTS/WLAN-first methods do in different mobility models. In addition, we investigate the accuracy of available bandwidth estimation, and the tradeoff between goodput and number of handoff.

It is noted that only two networks, WLAN and UMTS, are considered in our scheme. More types of network, such as WiMAX and WCDMA, will be integrated in our scheme. Moreover, we would like to adjust our approach for different traffic with different QoS.

References

1. Tripathi, N.D., Reed, J.H., Van Landingham, H.F.: Adaptive handoff algorithms for cellular overlay systems using fuzzy logic. In: Vehicular Technology Conference, 49th, vol. 2, pp. 1413–1418. IEEE, Los Alamitos (1999)
2. Park, H., Yoon, S.H., Kim, T.H., Park, J.S., Do, M.S., Lee, J.Y.: Vertical Handoff Procedure and Algorithm between IEEE 802.11 WLAN and CDMA Cellular Network. In: Mobile Commun. 7th CDMA Intl. Conf.

3. Roveri, A., Chiasserini, C.F., Femminella, M., Melodia, T., Morabito, G., Rossi, M., Tinnirello, I.: The RAMON Module: Architecture Framework and Performance Results. In: Proceedings of the Second International Workshop on Quality of Service in Multiservice IP Networks (2003)
4. Song, Q., Jamalipour, A.: Network selection in an integrated wireless LAN and UMTS environment using mathematical modeling and computing techniques. *Wireless Communications* 12(3), 42–48 (2005)
5. Ylianttila, M., Pande, M., Makela, J., Mahonen, P.: Optimization scheme for mobile users performing vertical handoffs between IEEE 802.11 and GPRS/EDGE networks. In: GLOBECOM 2001. Global Telecommunications Conference, vol. 6, IEEE, Los Alamitos (2001)
6. Ylianttila, M., Mäkelä, J., Pahlavan, K.: Analysis of handoff in a location-aware vertical multi-access network. *Computer Networks* (2005)
7. Makela, J., Ylianttila, M., Pahlavan, K.: Handoff decision in multi-service networks. Personal, Indoor and Mobile Radio Communications. In: PIMRC 2000. The 11th IEEE International Symposium (2000)
8. Salkintzis, A., Skyrianoglou, D., Passas, N.: Seamless multimedia QoS across UMTS and WLANs. In: Vehicular Technology Conference, VTC 2005-Spring. 2005, 61th, vol. 4, IEEE, Los Alamitos (2005)
9. Salkintzis, A.K., Dimitriadis, G., Skyrianoglou, D., Passas, N., Pavlidou, N.: Seamless continuity of real-time video across umts and wlan networks: challenges and performance evaluation. In: *Wireless Communications*, vol. 12(3), pp. 8–18. IEEE, Los Alamitos (2005)
10. Yang, X., Bigham, J., Cuthbert, L.: Resource management for service providers in heterogeneous wireless networks. In: *Wireless Communications and Networking Conference*, vol. 3, IEEE, Los Alamitos (2005)
11. Rajavelsamy, R., Jeedigunta, V., Holur, B., Choudhary, M., Song, O.: Performance evaluation of VoIP over 3G-WLAN interworking system. In: *Wireless Communications and Networking Conference*, vol. 4, IEEE, Los Alamitos (2005)
12. Ghini, V., Salomoni, P., Pau, G.: Always-best-served music distribution for nomadic users over heterogeneous networks. *Communications Magazine* 43(5), 69–74 (2005)
13. Shah, S.H.H., Chen, K.H., Nahrstedt, K.H.: Dynamic Bandwidth Management in Single-Hop Ad Hoc Wireless Networks. *Mobile Networks and Applications* 10(1), 199–217 (2005)
14. Shah, S.H., Chen, K., Nahrstedt, K.: Available Bandwidth Estimation in IEEE 802.11-based Wireless Networks. In: Proceedings of 1st ISMA/CAIDA Workshop on Bandwidth Estimation (BEst)
15. EURANE. Enhanced UMTS Radio Access Network Extensions for NS-2, <http://www.ti-wmc.nl/eurane/>

Self-authorized Public Key Management for Home Networks

Hyounghick Kim and S. Jae Oh

Home S/W Platform Team, Software Laboratory, Samsung Electronics
416, Maetan-3Dong, Yeongtong-Gu, Suwon-City, Gyeonggi-Do, Korea 443-742
{hyungsik.kim, sjae.oh}@samsung.com
<http://www.samsung.com>

Abstract. This paper describes the key management method which allows secure communication channels between devices in home networks. Home network technologies have developed to enable various kinds of home devices to access the digital information between the devices. Without security framework, however, the digital information including a user's private data may be exposed to a malicious attacker. Although conventional public key cryptosystems generally provide security features such as confidentiality and integrity, the distribution of the keys is vulnerable to man-in-the-middle attack without a trusted third party. In general home networks are dynamically set up without relying on any pre-existing infrastructure or central administration. Therefore, we must implement key distribution schemes without the assumption of a trusted third party. In this paper, we present self-authorized public key management for home networks. Our idea is to bind the device owner's authorization information to the public key of a device. Our protocol enables the distribution of the authenticated public key using an identity-based encryption scheme. We also provide heuristic analysis of various security properties.

Keywords: security framework, public key, home network, authorization, identity-based encryption.

1 Introduction

In recent years, the introduction of home networking technologies overcomes the barrier of sharing digital information in home. Consumer appliances such as TV, set-top box, mobile phone and digital camera have become tightly connected to each other through Internet based network connectivity. Many industrial standard organizations such as Digital Living Network Alliance (DLNA) [1], Home Audio-Video Interoperability (HAVi) [2], the Open Services Gateway Initiative (OSGi) [3] and Universal Plug and Play (UPnP) Forum [4] have made significant efforts to develop home network technologies. Home networks promise a major shift in our home. For example, a user watches some movie on the TV screen in the living room where the film is stored in set-top box in the bedroom and it is

rendered using the software in his children's PC. Without secure communication channel between devices, however, consumers may be skeptical about using the dreamy technologies of enabling the device connection for cooperative services. In particular, when home networks are connected to the Internet, the consumers will face even greater threats from a new class of Internet criminals who are likely to target home networks using Internet access to facilitate mayhem and mischief. Therefore, the security protection of such a networked appliance system will be expected as paramount to all others [13].

There are many security threats and vulnerabilities in home networks. In particular, a home-based wireless network may be more vulnerable to attacks such as eavesdropping without tapping cables since the technology's underlying communication medium, the airwave, is freely open to anyone. While wireless technologies such as IEEE 802.11 have made participating in the online world easier and more convenient, attackers can also intercept or modify the network traffics through the open communication channels. Unauthorized users may gain access to A/V services, corrupt a device's data, consume network bandwidth or capture the user's private information such as credit card number over the networks. Therefore, our work focuses on a wireless network which requires more secure procedures to defend against them.

For securing wireless networks, many solutions have been or are currently being developed. In particular, the IEEE 802.1X and 802.11i specifications identified several services to provide a secure operating environment. The three basic security services defined by IEEE for the wireless LAN environment are as follows [14]:

- Authentication: Authentication is to provide a security service to verify the identities of communicating devices. This provides access control to the network by denying access to client stations that is not authenticated.
- Confidentiality: Confidentiality is to protect the sensitive information against eavesdropping by intruders.
- Integrity: (Message) Integrity is to ensure that messages are not modified in transit between communicating devices.

An easy and secure setup of a wireless connection between communicating devices is a challenging issue in home-based wireless networks due to its characteristics of home users. Home-based wireless devices are usually installed by non-technical consumers and are often left in an insecure configuration due to a lack of knowledge. Effectively securing wireless devices such as router without assistance requires understanding several basic concepts in encryption and networking, and many consumers simply lack any form of training in these disciplines. Also, some consumers do not want to secure their devices since they do not understand the risks associated with an open node, while others understand the risk but judge the risk to be small enough to accept. A problem here is that many consumers do not aware that how the information that they do not protect may be abused due to the complicated impact of the threats. Currently, wireless network security is scarcely applied in a home. More than 80% of wireless network in a home is not using security features since people are having

difficulty in configuring AP despite a minimum user interactions such as typing a network identifier or a corresponding secret code [6]. Therefore, an innovative setup of security framework should be provided, which does not require troublesome user interactions and makes it easy to add and remove devices from the network.

In order to provide secure communication channels between devices, the devices must share secret session keys. The main problem is to distribute the session keys over initial networks which have not been securely configured. For the secure key distribution, it may seem strange that another secure channel is required for delivering keys again. Using Diffie-Hellman [19] or some other public key based key exchange [18] for this purpose, the problem of establishing shared keys over an insecure wireless channel is reduced to the problem of preventing a man-in-the-middle attack. In home-based wireless environment, it is possible that attacker can pose itself as a valid home device and participate in creating the secure session channel with other valid devices. The typical man-in-the-middle attack is described in Fig 1.

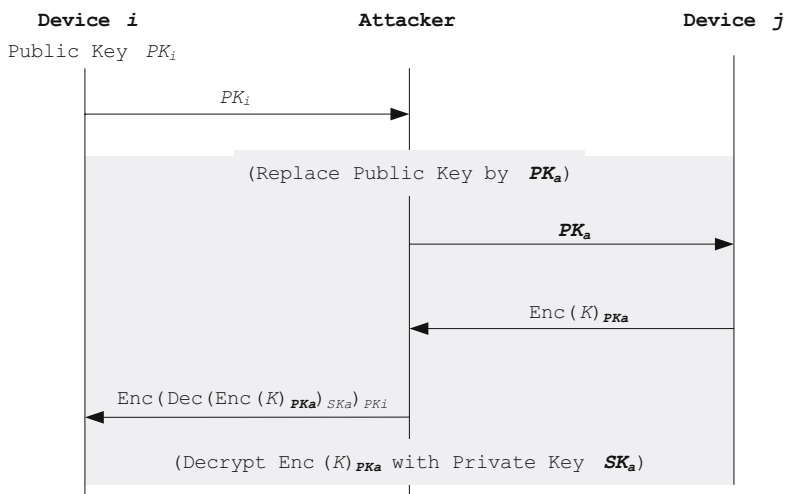


Fig. 1. Public Key Replacement

As shown in Fig 1, the attacker's device intrudes into the communication between the device i and the device j . The attacker captures device i 's public key and replaces the public key to the attacker's own public key as an intermediate network node by some method (e.g. DNS spoofing, ARP poisoning, etc).

To solve the above problem, the simplest approach is to use a trusted third party. The authenticated key distribution is achieved with the notion of certificate by a Certificate Authority (CA). For example, TLS [5] typically uses X.509 certificates [20]. In contrast with conventional networks, however, home networks

usually do not provide on-line access to CA or to centralized servers due to temporal disconnection to Internet or the limited capability of the client devices. For these reasons, traditional security solutions that require on-line CA or certificate repositories are not well suited for securing home networks. In this paper, we propose a fully self-organized public-key management system that allows home devices to generate their public-private key pairs and then to perform authentication without any centralized services. Furthermore, our approach does not require any trusted third party, not even in the network configuration phase. For this purpose, we assume existence of some out-of-band channel which human operators managed. The detailed information on the manual authentication protocols can be referred to [15] [16] [17].

In this paper, we propose a key management system using Identity-based encryption (IBE) [8] [9] [10] without a trusted third party. IBE is a useful tool for this purpose since it reduces the overhead for managing certificates. However, conventional IBE schemes still need a trusted third party for generating private keys and distributing public functions in a secure manner. Therefore we focus on the secure distribution of public parameters in a IBE scheme and the generation of private key without a third party.

To construct the authorized device's identifier, the proposed protocol uses a device owner's authorization information. One concern for this method is that the owner's authorization information is likely to be memorable information. Therefore, we should design the system which is protected against known dictionary attacks as one of our goals [11]. Also, a human operator's interactions must be minimized as much as possible. Our proposed solution enables users to use secure applications over home networks without managing any security mechanism.

The remainder of the paper is structured as follows: In section 2, we describe how the proposal was implemented. In section 3, we present some analysis of the proposed protocol. Finally, we conclude the paper and give an overview of future activities in section 4.

2 Protocol

In this section we propose a system for key establishment over home networks. We assume that there are two types of communication channels in home. The first one is an insecure, but high bandwidth communication channel between devices. In addition to this, a home device and the device owner share the other type channel which is a low bandwidth communication channel over which they can securely exchange the messages with the size of at most l bits. In practice, the human operator manually inputs data to a home device through the devices' input interfaces such as keypad. Operator-to-device transmissions are assumed to be secure.

In secure applications over home networks, devices try to share the common secret key by using two communication channels defined above. Without loss of generality, we assume that the size of the shared key is much bigger than the

maximum bandwidth l allowed by the low bandwidth communication channel since the device owner cannot manually inputs many data. Our proposed protocol is based on an IBE scheme for sharing secret key. Before getting into the protocol details, we will first introduce IBE scheme.

2.1 Identity-Based Encryption

An IBE scheme resembles an ordinary public key crypto system, involving a private and a public transformation. Instead of explicit public keys, the public key could be constructed from participant's publicly available information since an arbitrary string may serve as a valid public key. Conventional public keys are authenticated via certificates issued by a trusted certifying authority by binding participants' identities to the explicitly published public keys. The authenticity of the public keys provided by the signature of CA assures that only the entities hold their public keys. Therefore, in a certificate-based system, participants must verify other participants' certificates first before using their public keys. Consequently, a traditional public key crypto system requires a large amount of computing time and storage for managing keys and certificates. Shamir proposed the idea of IBE scheme in 1984 [7], but a practical fully-functional system was not found until recently by Boneh and Franklin [8]. Shortly after that, many identity-based cryptographic protocols were developed. In particular, the protocols based on pairings are currently an area of very active research [9][10].

In an IBE scheme, public key distribution ceases to be a concern since a participant's public key is simply a string that represents its identity. For example, a system has been developed where the email addresses are public keys. In this setting, a sender encrypts a message using a receiver's email address as the public key. Note that this can also be done offline. There is no need to look up, retrieve or verify public keys.

With IBE, the private keys are generally distributed by a trusted third party, often called the Private Key Generator (PKG). No private key can be computed without knowledge of a certain master secret, held only by the PKG. In contrast, public keys can be generated by any participants in the system. In practice, this master secret can be split among several PKGs. In this case, the system is compromised only if every PKG is successfully attacked. The detailed information on key management for IBE can be referred to [8][9].

For home networks, a natural approach based on IBE is to use the combination of the device owner's authorization information and the device identifier as a valid public key. We assume that the device owner holds the secret authorization information such as password for managing the home devices.

The advantages of using IBE to implement home networks layer security are readily apparent. No handshake, exchange of certificates, or verification of certificates is necessary as the devices can simply send a message encrypted with the public key computed using the authorization information in home. In this section, we describe how to construct our system from well-known IBE schemes.

2.2 Protocol Description

We construct the proposed protocol using the IBE scheme which Boneh and Franklin originally devised [8]. They used the bilinear maps relying on the Bilinear-Diffie-Hellman (BDH) assumption and the Random Oracle model [21] [22].

For using the IBE scheme, an elliptic curve group G_1 of prime order q and a finite field G_2 of prime order q with a bilinear mapping $e : G_1 \times G_2 \rightarrow G_2$, the bilinear mapping e and a generator P as the IBE scheme parameters, the master secret key $s_i \in_R \mathbb{Z}_q^*$ and the corresponding master public key $s_i \cdot P$ are embedded in the device i .

A device owner explicitly types a device identifier ID_i or use the default identifier which was initially installed into a device. After typing the device identifier, the owner securely stores the owner’s secret authorization information $auth$ with the size of l bits such as password in the device as one of authorized devices. The authorization information $auth$ is not stored in clear text but $g^{auth \cdot ID_i}$ using a generator g in a cyclic group G_3 of prime order q to protect the owner’s authorization information. For constructing common security framework in home, the information $auth$ must be identically applied to every device at home.

For exchanging sensitive information between the device i and the device j , a secure communication channel must be firstly created. Without loss of generality, we assume that the device j triggers the protocol. After receiving the request message for creating secure session channel, the device i instantly responses it with the master public key $s_i \cdot P$ and the device identifier ID_i to the device j . In home, these values can be distributed to all home devices through a specific message delivery mechanism such as the discovery protocol in a UPnP network.

After receiving the master public key $s_i \cdot P$ and the device identifier ID_i , the device j checks whether the communicating device is revoked. The device j searches the received device identifier ID_i in the revoked devices list. If the device identifier ID_i is found in the list, the device j stops communicating with the device i since the searched result means that device i is a revoked. Otherwise, the device j randomly chooses a symmetric session key K_{ij} and then computes the unique identifier for the communication with the device i using a random oracle H_1 as follows:

$$Q_{ij} = H_1((g^{auth \cdot ID_j})^{ID_i} || s_i \cdot P) \tag{1}$$

Here $H_1 : \{0, 1\}^* \rightarrow G_1$ is the random oracle and the value $g^{auth \cdot ID_j}$ has been initially stored in the device j . In the next step, the device j computes the mapping result g_i using Q_{ij} as follows:

$$g_i = e(Q_{ij}, s_i \cdot P) \tag{2}$$

The device j encrypts the key K_{ij} using g_i as follows:

$$Enc(K_{ij})_{PK_i} = \langle r \cdot P, K_{ij} \oplus H_2(g_i^r) \rangle, r \in_R \mathbb{Z}_q^* \tag{3}$$

Here $H_2 : G_2 \rightarrow \{0, 1\}^*$ is the random oracle. Finally the device j sends the encrypted symmetric session key $Enc(K_{ij})_{PK_i}$, the random number r , and

the device identifier ID_j through the insecure high bandwidth communication channel.

On receiving the message from the device j , the device i starts to decrypt the session key using the stored $g^{auth \cdot ID_i}$, the master secret s_i and the received message. The device i firstly computes Q_{ij} as follows:

$$Q_{ij} = H_1((g^{auth \cdot ID_i})^{ID_j} || s_i \cdot P) \quad (4)$$

Q_{ij} is clearly computed from the fact that $(g^{auth \cdot ID_j})^{ID_i}$ is the same as $(g^{auth \cdot ID_i})^{ID_j}$ due to the cyclic property of the group G_3 . The device i 's secret key SK_i is computed as $SK_i = s_i \cdot Q_{ij}$. The server extracts the symmetric session key K_{ij} from $\langle r \cdot P, K_{ij} \oplus H_2(g_i^r) \rangle$ using the server's secret key $s_i \cdot Q_{ij}$ as follows.

$$Dec(\langle r \cdot P, K_{ij} \oplus H_2(g_i^r) \rangle)_{SK_i} = K_{ij} \oplus H_2(g_i^r) \oplus H_2(e(s_i \cdot Q_{ij}, r \cdot P)) \quad (5)$$

By bilinearity property, $H_2(e(s_i \cdot Q_{ij}, r \cdot P))$ is the same as $H_2(e(Q_{ij}, s_i \cdot P)^r)$. That is, the decrypted result is computed as $K_{ij} \oplus H_2(g_i^r) \oplus H_2(g_i^r)$. Therefore, the device i and the device j share the symmetric session key K_{ij} and then can securely communicate with each other using the shared session key K_{ij} . In practice, some meaningful text must be appended into the session key K_{ij} to prevent against modification of the messages in the protocol. The device i can verify integrity of the previously received $Enc(K_{ij})_{PK_i}$, r , and ID_j from the device j by checking whether the appended text is regularly decrypted without trouble.

According to circumstances, the device i and the device j may confirm each other's knowledge of the symmetric session key K_{ij} . One way is to exchange the encrypted r with the agreed symmetric session key K_{ij} .

It is intuitive to prove that the proposed protocol is correct in the sense that the participating devices in the construction of a secure communication channel are guaranteed to agree on a common session key if the valid authorization information is predefined by the device owner.

2.3 Revocation

The device owner should be able to revoke a device when it is lost or stolen. In our protocol, the revocation mechanism is very simple and efficient. The owner simply adds the information of revoked device to the revoked devices list without changing the owner's authorization information. The owner explicitly types the revoked device's identifier. This value is added to the revoked device list.

3 Analysis

In this section, we show that the proposed protocol satisfies the security properties in home networks. The general information on the security properties for home networks can be referred to [12].

It may be difficult to show the proposed protocol is formally secure. In general, the formal security analysis requires many assumptions in the context of the adversary models. In general terms, an attacker, who is defined here as a malicious third party interested in subverting communication between home devices i and j , must not be able to obtain the meaningful information of the symmetric session key K_{ij} or the device owner's authorization information $auth$ by observing the messages exchanged during a successful run of the protocol or modifying them. Most requirements are directly satisfied by a cryptographically secure IBE scheme.

For confidentiality, it is apparently impossible to eavesdrop the symmetric session key K_{ij} which is encrypted with the device i 's public key PK_i . The secrecy of the key K_{ij} is protected unless the device i 's the secret key SK_i is computed. For computing it, an attacker needs the device i 's the master secret key s_i . The computational infeasibility of s_i is based under a secure IBE scheme. Also, no useful information about the owner's authorization information $auth$ is revealed during the successful run of the protocol since the computed results with $auth$ as input are not exposed to the attacker. Therefore, the proposed protocol is also secure against the dictionary attack.

For a device authentication, it is apparently impossible to masquerade as a valid home device using an attacker's device. In the view of device i , the attacker cannot compute Q_{ij}' in the equation (4) without $g^{auth \cdot ID_i'}$, when the attacker wants to forge the master public key $(s_i \cdot P)'$ or the device identifier ID_i' without regard to the device owner's authorization information $auth$. Also, in the view of device j , the computation of valid Q_{ij}' is also impossible without $g^{auth \cdot ID_j'}$ in the similar manner. The only attack is to guess the owner's secret authorization information $auth$. In this way, the attacker successfully guesses it with probability $\frac{1}{l}$ when $auth$ is randomly selected. Therefore the attacker cannot intrude into the communication with the construction of secure session channel with valid home devices under some assumptions.

In home environment, however, devices may be corrupted by an attacker since the devices can be lost or stolen. Therefore, we need to consider some additional requirements defined in the group key management protocols [23].

For forward secrecy, it is also impossible to compute SK_i even if an attacker holds the device i 's the master secret key s_i . The attacker may try to construct a secure session with other valid home devices through the stolen device. For avoiding the test of revoked devices, the attacker must use a new device identifier ID_a . Given values $g^{auth \cdot ID_i}$, ID_i and ID_a , however, the attacker cannot efficiently compute $g^{auth \cdot ID_a}$ since $g^{auth \cdot ID_i}$ is the same as $(g^{ID_i})^{auth}$. Therefore, it is secure under the assumption of computationally infeasibility to the discrete logarithm problem.

For key Independence, the public-private key pair per session is used instead of group key mechanism. Clearly, this approach is more useful for home environment since sharing of the group key may intrude on a user's privacy.

4 Conclusion

In this paper, we have presented a new security framework based on IBE schemes for home networks.

To construct a secure channel between authorized devices, the proposed protocol provides authenticated key distribution. Our approach, which is based on an IBE scheme, satisfies security requirements for home environment. We generate a valid public key which is associated with the device owner's authorization information. By this way a secure channel can be simply constructed. No other mechanism for authenticating the exchanged public key is necessary while conventional methods need a trusted third party.

We expect that the proposed protocol provides a reasonable level of security against attacks related to applications over home networks. In practice, our proposed protocol can be used for many applications such as e-commerce, home shopping and health care over home networks.

It would be interesting to extend to the construction of secure group communication consisting of n devices. Secure group communication is designed to provide a pool of devices communicating over a public network with a session key. In the future, we plan to investigate how our system can be efficiently extended. We will also investigate a formal security proof of the system.

References

1. DLNA: DLNA Overview and Vision (2006), http://www.dlna.org/en/industry/about/dlna_white_paper_2006.pdf
2. HAVi: HAVi, the A/V digital network revolution (1999), <http://www.havi.org/pdf/white.pdf>
3. Marples, D., Kriens, P.: The Open Services Gateway Initiative: An Introductory Overview. *IEEE Communications Magazine*, 110–114 (2001)
4. Miller, B.A., Nixon, T., Tai, C., Wood, M.D.: Home Networking with Universal Plug and Play. *IEEE Communications Magazine*, 104–109 (2001)
5. Dierks, T., Allen, C.: The TLS Protocol ver. 1.0. RFC 2246 (January 1999), <http://www.ietf.org/rfc/rfc2246.txt>
6. Tsang, P.: APEC TEL wireless (802.11) security, workshop: Nextsteps. In: APEC TEL Conference (2004)
7. Shamir, A.: Identity-based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) *CRYPTO 1984*. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
8. Boneh, D., Franklin, M.: Identity-based Encryption from the Weil pairing. In: Kilian, J. (ed.) *CRYPTO 2001*. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
9. Gorantla, M.C., Gangishetti, R., Saxena, A.: A survey on id-based cryptographic primitives. *Cryptology ePrint Archive*, Report 2005/094 (2005), <http://eprint.iacr.org/>
10. Dutta, R., Barua, R., Sarkar, P.: Pairing-based cryptographic protocols: A survey. *Cryptology ePrint Archive*, Report 2004/064 (2004), <http://eprint.iacr.org/>
11. Jablon, D.P.: Strong Password-Only Authenticated Key Exchange. In: *ICM SIG-COMM Computer Communication Review*, vol. 26, ACM Press, New York (1996)

12. Ellison, C.M.: Home Network Security. Intel Technology Journal 6 (November 2002), <http://developer.intel.com/technology/itj/index.htm>
13. Moyer, S., Marples, D., Tsang, S.: A Protocol for Wide-Area Secure Networked Appliance Communication. IEEE Communications Magazine 6, 52–59 (2002)
14. Karygiannis, T., Owens, L.: Draft: Wireless Network Security - 802.11, Bluetooth and Handheld Devices. USA. National Institute of Standards and Technology (2002)
15. Gehrman, C., Mitchell, C.J., Nyberg, K.: Manual authentication for wireless devices. RSA Cryptobytes 7(1), 29–37 (2004)
16. Vaudenay, S.: Secure communications over insecure channels based on short authenticated strings. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 309–326. Springer, Heidelberg (2005)
17. Hoepman, J.-H.: Ephemeral pairing on anonymous networks. In: Hutter, D., Ullmann, M. (eds.) SPC 2005. LNCS, vol. 3450, pp. 101–116. Springer, Heidelberg (2005)
18. Rivest, R.L., Shamir, A., Adleman, L.M.: A Method for Obtaining Digital Signatures and Public-key Cryptosystem. Communications of the ACM 21, 120–126 (1978)
19. Diffie, W., Hellman, M.E.: New Directions in Cryptography. IEEE Transactions on Information Theory IT-22, 644–654 (1976)
20. Housley, R., Ford, W., Polk, W., Solo, D.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Internet Standard. RFC 2459, The Internet Society (1999)
21. Bellare, M., Rogaway, P.: Random Oracles are Practical: a Paradigm for Designing Efficient Protocols. In: Proceedings of ACM CCS 1993 (1993)
22. Canetti, R., Goldreich, O., Halevi, S.: The Random Oracle Methodology, Revisited. In: Proceedings of Symposium on the Theory of Computing, ACM, New York (1998)
23. Kim, Y., Perrig, A., Tsudik, G.: Simple and fault-tolerant key agreement for dynamic collaborative groups. In: Proceedings of ACM CCS 2000 (November 2000)

A Cross-Layered Diagnostician in OSGi Platform for Home Network

Pang-Chieh Wang, Yi-Hsuan Hung, and Ting-Wei Hou

Dept. of Engineering Science, National Cheng-Kung University,
Tainan, Taiwan
{pangchieh, elegance, hou}@nc.es.ncku.edu.tw

Abstract. The service gateway in a home network plays an important role as a centric service controller. New services can be updated and plugged by the operators or users of the gateways. But more services in the gateway bring more complex service relations and may bring some unexpected exceptions and conflicts. This research summarizes the requirements of diagnosis in open service platforms and integrates several techniques to develop a cross-layer approach for detecting the service conflict fault, handling the general exceptions, and diagnosing the device fault on OSGi platforms. This solution, called Diagnostician, helps users and operators handle the problems in OSGi and reconfigure the system.

Keywords: Service gateway, OSGi, diagnosis, cross-layered.

1 Introduction

There are a lot of emerging researches on the digital home and smart appliances. Based on the technologies of home networking, more and more smart appliances are connected in the home networks. They are able to communicate and cooperate with each other through the home gateway. The Open Service Gateway initiative Alliance [12] defines such a service-oriented and component-based platform called OSGi Service Platform. With the OSGi technology, one complicated job which requires controlling several devices can be done automatically.

With the increasing number of services for improving the user's daily life, the user would feel more convenient to enjoy the benefits of these services. Unfortunately, the complexity of operating these networked smart devices also increases significantly, which make users spend more time figuring out how to set them up, what functionality they can do, and how to keep them working [5]. Moreover, common users do not know how to troubleshoot the services when they encounter some faulty situations such as the network is jammed, the service works inappropriately, or the gateway seems to be broken, etc. Hence the robustness of the open service platform becomes one of the major concerns of residents in smart homes [3].

In addition, most faults except hardware problems are due to the inappropriate operations of the user while assuming that the services are trustworthy. Since all the members in a family will request to access the resources in the digital home, the

operations of distinct services may conflict when they need to access a device at the same time. If these inappropriate operations are collected in advance and maintained by the service providers, this kind of faults can be prevented before the problem occurs rather than diagnose such problems after the user has lost his/her patience.

The exceptions also occur in the service platform and require an exception handling mechanism for detecting and resolving them. Although each service should have its own exception handling mechanism, there should be a general exception handling mechanism at the higher level of a service platform. Thus the general exceptions such as installing service failed, stop service failed, and so on can be handled, even resolved automatically, by the service platform.

In order to resolve the above faulty conditions, we propose a cross-layer approach on the OSGi platforms for detecting conflict(s) between distinct services. The high level exception handling mechanism is also addressed on the OSGi platform. In addition, the on-demand diagnostician embedded in an OSGi platform is able to assist the user when he/she encounters some problems in operating the services.

In section 2, we categorize the problems about the diagnostician would encounter in the service gateway and some other researches are introduced, too. The design of the proposed diagnostician in the service gateway and some results are presented in section 3. The last is the conclusion and future work in section 4.

2 Related Works

Here we categorized the problems of services gateways and indicates the characteristics of each problem.

2.1 Challenges on Fault Diagnosis

The issues of software debugging and fault diagnosis are often taken into consideration as designing various kinds of computing systems like operating systems, embedded or distributed systems, and network computing, etc. Each of these computing systems would define different kinds of challenges it would face, respectively. To design a fault diagnosis model on an open service framework, the challenges of fault tolerant pervasive computing defined in [14] can be applied. The authors in [14] discuss four fault tolerant issues:

1. **Fault Detection:** It is a difficult problem to do an effective fault detection task in a pervasive computing environment. In a common way, the device or application can be periodically checked to see if it is alive such as heartbeat messages. The drawback is that plenty of devices and applications make the data traffic of the heartbeat messages increases significantly.
2. **Fault Containment:** The fault that has been detected needs to be solved or isolated right away to block the spread of more serious faults. This is a critical problem, especially in the pervasive computing environment, since there are many services work together. A job would not terminate and even get worse if one service is down causes the other services operate incorrectly.

3. **Transparent Fault Tolerance:** One of the key characteristics of pervasive computing is transparency [16]. The pervasive system should mask all the faults and try not to disturb the user. In other words, the system needs to decrease the user's awareness as much as possible.
4. **Good Fault Reporting Mechanisms:** The system needs to report the fault information and suggest a solution to the user whenever a fault has been detected regardless of whether this fault can be solved automatically or not. Something needs to be noticed is how to report to the user in some kind of non-intrusive ways.

2.2 Exception Handling

The conditions which are brought to the attention of the operation's invoker while attempting to perform some operations are called exception conditions [6]. Then the invoker needs to respond to the conditions. The operation of bringing an exception condition to an invoker's attention is called raising an exception. Handling the exception is defined as the invoker's response. An exception condition would make the system inconsistent and may result in system failure.

The services of open service framework are increasing in a significant speed. The number of exceptional conditions is incident to various services. In order to enhance the robustness, fault tolerant techniques are introduced. One of the most important schemes for detecting and recovering errors is the exception handling mechanism [4]. The exception handling mechanism could also be used for structuring fault-tolerant activities in a system. Exception handling [2] is an acknowledged technique to ensure fault tolerance in a system which is up against a variety of faults [1].

2.3 Avoidance of Service Conflicts

The services on the OSGi framework are able to access and control home appliances such as televisions, telephones, and surveillance cameras, etc. If there are multiple services invoked by different users trying to access the same resource at the same time, a service conflict problem would occur because the resource is not available. Neither OSGi framework nor the service itself can handle such an unexpected error. Thus service mediation is necessary because there are various services running on one gateway operated by multiple users, which results in service conflict problem [11].

A common solution is to set priority. A rule-based controlling framework for a context-aware system [9] avoids the conflict to each device by simply setting and checking the priority. A conflict occurs when multiple rules indicating that different actions are required for the same device. The framework provides a mechanism to detect a conflict among multiple rules automatically. Thus the appropriate operation is chosen according to the predefined priority.

Since the context used to determine the priority is fixed, the process of service control is uniform such as certain service always gets higher priority. This is not appropriate for avoiding device conflicts [10]. Thus Ogawara, Kobayashi et al. develop a service control platform for the user-oriented home network services called "Home Service Harmony" [10]. The system estimates the importance of each service according to the user's preference and the usage history. The resources are assigned to services in accordance with the importance of each service. Because the importance is changing

during runtime, the conflicts among resources can be avoided dynamically. However, as they comment, the system is difficult to handle controls if there are several users trying to use the same service. This is a significant drawback for applying this mechanism to an open service environment with multi-users.

We separate the above researches into three groups in Table 1 and highlight the techniques applied in these researches. The first group, called Fault Diagnosis Group, contains the fault diagnosis models discussed in section 2.1. The second group, called Exception Handling Group, includes all the exception handling approaches discussed in section 2.2. The researches discussed in section 2.3 are contained in the Service Conflict Avoidance Group. If there is a check sign, it means that the works in this group have the functionality described in the left column of this row. Otherwise the functionality is not supported. In addition, there are several functionalities which are not supported by all the researches in a group, i.e. only some are able to do that job. A triangle sign is used to describe this kind of incomplete conditions.

Table 1. A comparison between the related researches

| | Fault Diagnosis Group | Exception Handling Group | Service Conflict Avoidance Group |
|--|------------------------------|---------------------------------|---|
| Fault Detection | √ | N/A | N/A |
| Fault Correction | √ | N/A | N/A |
| Fault Reporting | △ | N/A | N/A |
| Exception Handling | N/A | √ | N/A |
| Exception Reporting | N/A | √ | N/A |
| Resource Access Conflict Avoidance | N/A | N/A | √ |
| Human Behavior Conflict Avoidance | N/A | N/A | △ |
| √: All the researches in this group support the functionality. | | | |
| △: Not all the researches in this group support the functionality. | | | |

3 Design and Implementation

3.1 Design of Diagnostician

Diagnostician is designed on the OSGi framework to solve the problems discussed in previous sections. The architecture of the whole framework is shown in Fig. 1. The Original Component blocks refer to the components that the OSGi framework originally have. We embed the Automated Logging Framework (ALF, one of Major Component blocks) between OSGi framework and Java Virtual Machine (JVM) to catch all the method invocation events triggered from JVM. There is a Conflict Detector (one of Sub Component block) inside ALF to monitor the OSGi service activities.

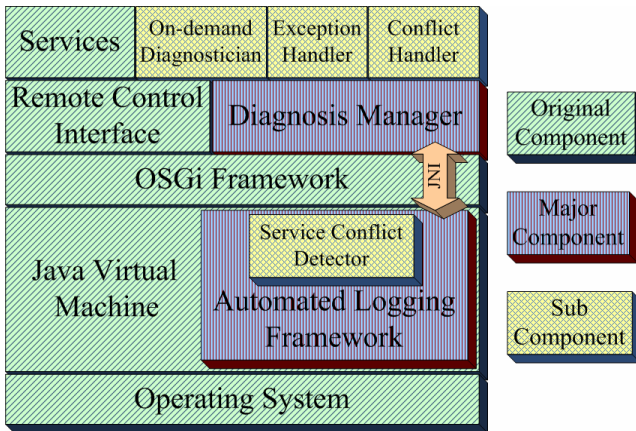


Fig. 1. The architecture of proposed Diagnostician

In the upper layer, the Diagnosis Manager (another Major Component block), which is an OSGi bundle, manages all the faults. It is the manager of the three sub components: On-demand Diagnostician, Exception Handler, and Conflict Handler. Each component handles one kind of faults. In addition, the On-demand Diagnostician is embedded in the original remote control interface and managed by the Diagnosis Manager. Diagnostician is able to assist the user when he/she encounters some problems like the occurrence of unexpected operations or device error. The following paragraphs show the details of the design concept and the implementation of each component.

- **Diagnosis Manager**

The Diagnosis Manager bundle manages all the faulty situations with the upper sub-component as On-demand Diagnostician, Exception Handler, and Conflict Handler. This bundle is a two-way bridge between the OSGi framework and all the fault detectors. It could not only communicate with the fault detector in native JVM level, but also perform the administrative actions on the OSGi framework like stopping an illegal bundle, showing some human-readable messages, and so on.

- **Conflict Detector**

As several services need to access and control the same device concurrently on the OSGi platform, it is like the ‘race condition’ which is a classical issue in process synchronization of operating systems [7]. We found that this problem would happen on OSGi platform. To take precautions against the race condition, we have to ensure that only one service/method at a time can access the device/resource. The solution to the critical-section problem [7] is taken into consideration. When the device is in use, no other related methods are allowed to get the control of the same device. Thus, this device controlled by one service is “mutually exclusive”.

- **Modified ALF**

The tool, Automated Logging Framework (ALF), is used to help catching the event of method entry. ALF is modified to have the conjunction of OSGi platform and itself. Thus ALF can notify the Diagnosis Manager to do some operations on OSGi platform when a mutually exclusive service is detected. In order to communicate between ALF (implemented in standard C++) and OSGi framework (implemented in JAVA), some JNI (Java Native Interface) calls are added. Thus ALF could set the bundle ID of the newly loaded class while handling a class load event.

3.2 Implementation Result

We implemented the proposed Diagnostician on the OSGi framework to verify our solutions to handle the faults. The components of the prototype are listed in Table 2. The Knopflerfish 2 [7], the open source implementation of OSGi framework Release 4, is used. The version of JVM is J2SE 1.4.2 running on Windows XP. The remote control interface is modified from the httpconsole bundle developed by Knopflerfish. A user can access the remote control interface via Internet since a web server on the OSGi platform is activated. In addition, ALF is used as a tool for catching JVM events.

Table 2. A prototype

| Software | Name or Version | Hardware | Information |
|-----------------------------|------------------------------------|------------------|-------------------|
| Operating System | Windows XP Pro. | CPU | Intel Pentium M |
| Java Virtual Machine | J2SE 1.4.2 | Clock | 1.73 GHz |
| OSGi Framework | Knopflerfish 2 (OSGi Release 4) | Hard Disk | 60 GB 4200 rpm |
| Network | Ethernet 1Gbps | Memory | 1G ram |
| Web Server | Knopflerfish Http Server | | |
| Additional Tool | Automated Logging Framework | | |

The exceptions may occur anytime. In a scenario, we assume that the user had successfully installs the 'Serial Port Device' service on the prototype OSGi framework. The remote control interface shows the messages which are responses from the OSGi framework. After starting this bundle, the messages shown in Fig. 2 indicating that an exception occurs because of missing a package called 'javax.comm'. The exception handler then finds and installs the necessary bundle automatically. Thus the user can start the Serial Port Device bundle again successfully without the occurrence of exceptions.

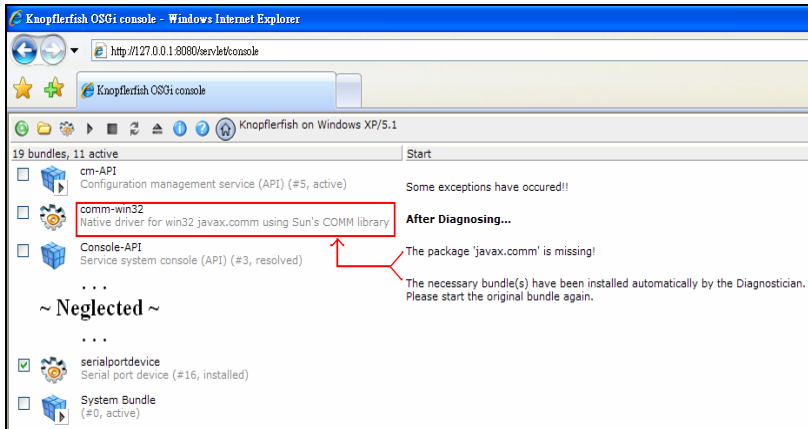


Fig. 2. The snapshot after diagnosing the exception

If the user finds out that the milk box is actually empty and doubts that the Refrigerator service may have some problem, he/she can click the button in the square of Fig. 3 to activate the On-demand Diagnostician. After the diagnosing has been done by downloading and starting a corresponding diagnosing bundle, the final result of the diagnosing process is shown on the right side of the screen as illustrated in Fig. 3. Therefore, the user can figure out what may be broken.

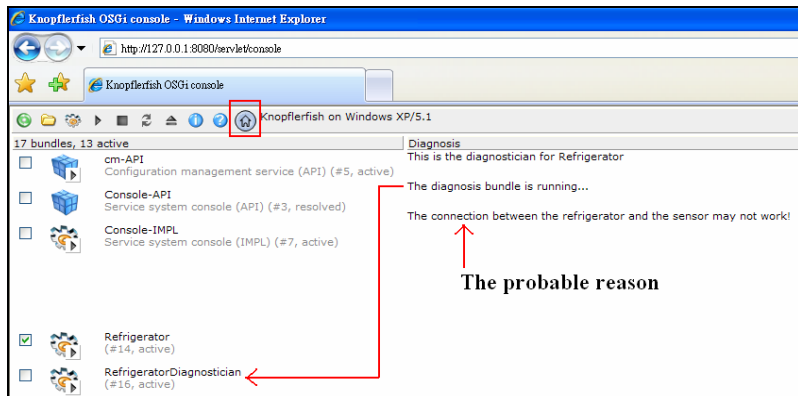


Fig. 3. The snapshot after performing the On-demand Diagnostician

For another example, a service conflict may occur as the mother wants to take a picture by the camera, controlled by Home Surveillance Service, via the link of remote control interface. If there is not any conflict, the snapshot would be taken and shown on the web page. Otherwise the conflict fault would be detected and this service becomes unavailable because the Diagnosis Manager would stop it. The picture is unavailable and the messages are shown in Fig. 4.

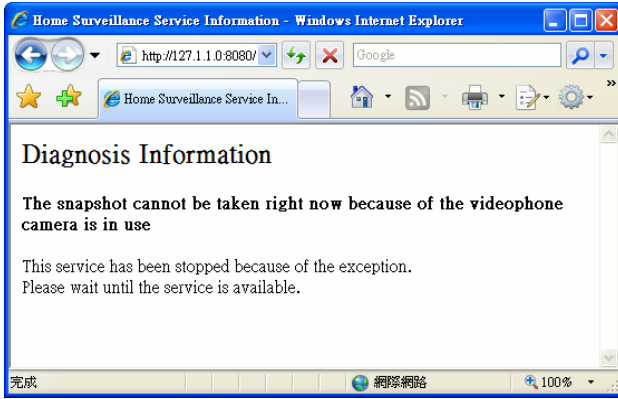


Fig. 4. An example of diagnosis information

We evaluate the execution time when handling exceptions in different conditions and show the result in Fig. 5. The plain OSGi is without our Diagnostician and the time means an exception occurs then the service stopped. After installing it, an exception occurred with our Diagnostician catching and handling it. It takes 7.6ms and 9.95ms while showing the message on the user interface. The performance of the proposed solution seems not good because the ALF takes time in filtering and analyzing the information. In realistic, the time is still short enough to make user accept it. If there is not a Diagnostician in the service gateway, the plain OSGi cannot suggest and locate the possible reason of the exception, which would require a user or an operator spend a lot of time to find it out.

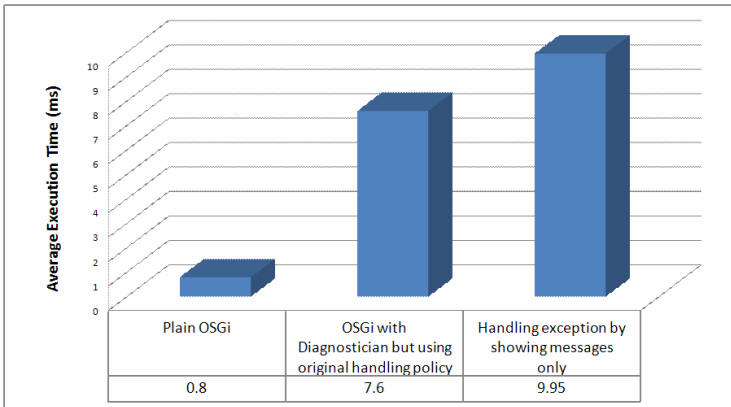


Fig. 5. The performance evaluation of the Diagnostician

4 Conclusion and Future Work

The robustness of an open service platform is a critical issue. End users applying the smart home technology to their current houses look forward to improving their lives in

a more convenient way, rather than bringing more troubles in dealing with the complex services and faulty situations frequently like some fault scenarios in this research. A cross-layer approach is proposed for detecting the fault(s) of service conflict(s) and handling the general exceptions on OSGi platforms. The OSGi platform with the proposed cross-layer approach is able to detect the service conflict fault in advance while the operations of distinct services called by different users conflict with each other. The general exceptions, caused by some inappropriate operations of a user, are handled as well. Both of the faults are resolved automatically without the user's awareness. The user would receive the human-readable information, which describes the faulty situation and what solutions have been done, shown on the user interface such as the web page. Furthermore, an on-demand Diagnostician module can be triggered by the user when he/she encounter some problems in the reaction of some probably faulty devices. The on-demand Diagnostician then installs the corresponding diagnosis bundle and begins to analyze the specified service and/or device. The results and suggestions are provided to the user for figuring out what service is crashed or what device is broken.

The advantages of the proposed approach is that the end users would be pleased without being bothered about the faulty situation, the service providers would discover that the requests for technical supports are reduced, and the service designers would take their ease with developing new services without caring about the operations may conflict with other existing services.

The current approach only focuses on the faults of service conflict and exception. Other fault tolerance techniques like auto reconfiguration and security issues would be considered in the future. More complete exceptions would be included in the exception handler rather than the general exceptions only. The interface for presenting the detailed information would be improved in a more user-friendly way and applied in various devices such as TV display, mobile phone, and so on.

References

1. Budi, A., Alexei, I., Alexander, R.: On Using the CAMA Framework for Developing Open Mobile Fault Tolerant Agent Systems. In: Proceedings of the 2006 International Workshop on Software Engineering for Large-Scale Multi-Agent Systems, pp. 29–36. ACM Press, Shanghai, China (2006)
2. Cristian, F.: Exception Handling and Software Fault Tolerance. *Transactions on Computers* C-31, 531–540 (1982)
3. Edwards, W.K., Grinter, R.E.: At Home with Ubiquitous Computing: Seven Challenges. In: Abowd, G.D., Brumitt, B., Shafer, S. (eds.) *Ubicomp 2001: Ubiquitous Computing*. LNCS, vol. 2201, pp. 256–272. Springer, Heidelberg (2001)
4. Garcia, A.F., Rubira, C.M.F., Romanovsky, A., Xu, J.: A Comparative Study of Exception Handling Mechanisms for Building Dependable Object-Oriented Software. *Journal of Systems and Software* 59, 197–222 (2001)
5. Grinter, R., Edwards, W., Newman, M., Ducheneaut, N.: The Work to Make a Home Network Work. In: *ECSCW 2005. Proceedings of the 9th European Conference on Computer-Supported Cooperative Work*, pp. 469–488. Springer, Netherlands (2005)
6. John, B.G.: Exception Handling: Issues and a Proposed Notation. *Communications of the ACM* 18, 683–696 (1975)

7. Knopflerfish Project: Open Source OSGi Framework Implementation, <http://www.knopflerfish.org/>
8. Leslie, L., Robert, S., Marshall, P.: The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4, 382–401 (1982)
9. Nishigaki, K., Yasumoto, K., Shibata, N., Ito, M., Higashino, T.: Framework and Rule-based Language for Facilitating Context-Aware Computing using Information Appliances. In: 25th IEEE International Conference on Distributed Computing Systems Workshops, Columbus, Ohio, USA, pp. 345–351 (2005)
10. Ogawara, M., Kobayashi, E., Yoda, I.: Home Network Service Management Technologies. *NTT Technical Review* 3, 17–21 (2005)
11. Okugawa, T., Masutani, H., Yoda, I.: A Home Network Service Environment for Wide-Area Communications. In: *Proceedings of 2005 Asia-Pacific Conference on Communications*, Perth, Western Australia, pp. 14–18 (2005)
12. OSGi Alliance: Open Service Gateway Initiative Technology, <http://www.osgi.org/>
13. Sara, B., Bill, S., David, W.M., Barbara, R., Ylian, S.-H.: Broken Expectations in the Digital Home. In: *CHI 2006. Conference on Human Factors in Computing Systems extended abstracts on Human factors in computing systems*, pp. 568–573. ACM Press, Montréal, Québec (2006)
14. Shiva, C., Anand, R., Campbell, R.: Towards Fault Tolerance Pervasive Computing. *IEEE Technology and Society Magazine* 24, 38–44 (2005)
15. Utton, P., Scharf, E.: A Fault Diagnosis System for the Connected Home. *IEEE Communications Magazine* 42, 128–134 (2004)
16. Weiser, M.: The Computer for the 21st Century. *Scientific American* 265, 94–104 (1991)

LaMSM: Localization Algorithm with Merging Segmented Maps for Underwater Sensor Networks

Eunchan Kim, Seok Woo, Chungsan Kim, and Kiseon Kim

Department of Information and Communications,
Gwangju Institute of Science and Technology (GIST),
1 Oryong-dong, Buk-gu, Gwangju, 500-712, Republic of Korea
{tokec, swoo, only2442, kskim}@gist.ac.kr

Abstract. Underwater sensor networks (UWSNs) are considered a cost-effective solution to ocean applications, such as the acquisition of natural resources in oceans, protection from underwater disasters, etc. These applications basically require location information of nodes to identify the venue of reported events. To locate more accurately the position of nodes, multidimensional scaling (MDS) is widely used because of its good tolerance to errors in measured distances. MDS requires measured distances between every pair of nodes but in practice, only distances between nodes within a communication range can be measured. Hence, the well-known MDS-MAP(P) [6] calculates unmeasured distances for MDS but these calculations result in large errors. In this paper, we proposed a localization algorithm with merging segmented maps (LaMSM) that constructs many reliable segmented maps composed of only nodes within a communication range, and then merges them together based on their common nodes. The segmented maps are built from only the measured distances and as a result, LaMSM provides more accurate node positions than MDS-MAP(P).

Keywords: sensor networks, optimization, localization, multi-dimensional scaling.

1 Introduction

Recently, many countries have been turning their interest toward underwater applications to acquire natural resources in oceans, to monitor pollution, to prevent disasters, etc. For such applications, there are many underwater systems using autonomous underwater vehicles (AUVs) which explore and gather geological features from the ocean floor. However, traditional underwater devices usually have difficulties in real-time monitoring, high expense, and recovery from failure. To overcome these difficulties, underwater sensor networks (UWSNs) are emerging as a cost-effective solution by monitoring events near sensor nodes deployed underwater [1]. The major difference between UWSNs and terrestrial sensor networks is the communication channel among sensor nodes. Due to the

limited transmission range of high radio frequency (RF) signals, acoustic signals are alternatively used for UWSNs because of their long transmission range: up to 1Km, 10Km, and 100Km depending on the used bandwidth and frequency.

Acoustic signals experience high delays due to the low speed of sound underwater: about 1.5×10^3 m/s [12]. High delays of acoustic signals can provide more accurate distances between nodes through resolving the delays called time of flight (ToF) than in the case of RF signals. Once distances between nodes are secured, sensor nodes can be localized with useful traditional localizations. Among the basic methodologies for localization, multidimensional scaling (MDS) is a popular mathematical tool due to its good tolerance to errors in measured data. MDS computes the positions of nodes from both connectivity and distance between nodes [3]. Applying MDS to localization needs distance information between every pair of nodes in a network but in practice, a node can measure only the distances to nodes within a communication range.

For complete distance information, MDS-MAP calculates the unmeasured distance by summing measured distances along the shortest multi-hop path between nodes [4]. It then constructs a global map where all nodes are located and relocates the global map with the given beacon nodes. However, errors in calculating the unmeasured distance becomes greater as the number of hop counts in the shortest path increases, which considerably affects the localization error of nodes. To patch MDS-MAP, MDS-MAP(P) restricts the hop count to 2 or 3 hops in calculating unmeasured distances, which prevents errors in distances from increasing [5,6]. Hence, MDS-MAP(P) first builds local maps for 2-hop or 3-hop areas and then merges them together to construct a global map. It performs well but there are still open problems to improve accuracy: how to obtain more accurate local maps and how to merge them with minimum error.

In this paper, we propose a localization algorithm with merging segmented maps (LaMSM) which constructs segmented maps with only fully connected nodes, merges segmented maps to build a local map, and merges local maps again to form a global map. Because the segmented maps are the basic units for a global map, it is important to reduce localization error in a segmented map. To build a reliable segmented map with MDS, LaMSM uses only measured distances by grouping only the nodes fully connected to one another. The rest of this paper is organized as follows: Section 2 summarizes literature related to our current research, Section 3 explains our proposed algorithm in detail, and Section 4 presents the simulation results under varying errors in distance measurements. Finally, we conclude this paper in Section 5.

2 Related Works

In this section, we explain several distance-based localizations that construct a local map with measured distances and then merge them together. These are well known for their good performance using a small number of beacon nodes.

MDS-MAP(P) proposed by Shang et al. [5] uses multidimensional scaling (MDS) and local distance information. Most local distances between nodes can

be obtained by resolving received packets but there still remain unmeasured distances in a local area. Building local maps with the MDS requires fully complete distance information for all nodes in a local area so that MDS-MAP(P) calculates the sum of measured distances along the shortest path between two nodes instead of unmeasured distances.

Moore et al. presented a distributed localization which constructs robust quadrilaterals for local maps and merges them together [7]. The quadrilateral is constructed with a trilateration method using distances among four nodes. When two quadrilaterals are merged, a map is sometimes reflected and merged into another map because of a serious position error in quadrilaterals called flip ambiguity. To prevent flip ambiguity, Moore et al.'s scheme collects only robust quadrilaterals in which four nodes should have full connections to one another and greater than a pre-defined angle between them. This restriction could reduce the possibility of flip ambiguity but it also excludes the chance for other node maps to be used as quadrilaterals. Only robust quadrilaterals are merged together using the closed-form solution suggested by Horn et al. [9].

While the previous localizations take into consideration local map construction with constraints and basic mathematical tools, e.g., MDS or trilateration, Kwon et al. turned their focus to a merging method to overcome flip ambiguity in their localization [8]. They utilized a merging method based on the closed-form solution of Horn et al. and additional distance information. In addition, they investigated performance between maps with the MDS method and the multilateration. According to their results, merging MDS-based local maps shows better localization accuracy than merging multilateration-based local maps. However, the MDS-based local maps are constructed with the same mechanism as the MDS-MAP(P), so that the local maps also have errors due to the calculated distances as well as errors due to measurement error.

3 Proposed Localization Algorithm

This section discusses the causes of localization inaccuracy of local maps in MDS-MAP(P) and describes the proposed localization algorithm which also follows the overall structure of MDS-MAP(P) but adopts different mechanisms to construct local maps and to merge them.

3.1 Problem Statement

Building a local map with MDS, MDS-MAP(P) calculates all distances between every pair of nodes within a local area by summing the measured distances along the shortest path between them. In the calculated distance between distant nodes, errors arising from indirect paths degrade the accuracy of nodes' positions in a local map rather than errors in measurements. Fig. 1(a) shows the real deployment of node 1 and its neighbors, where a line between two nodes stands for a direct connection. For instance, node 2 cannot directly communicate with

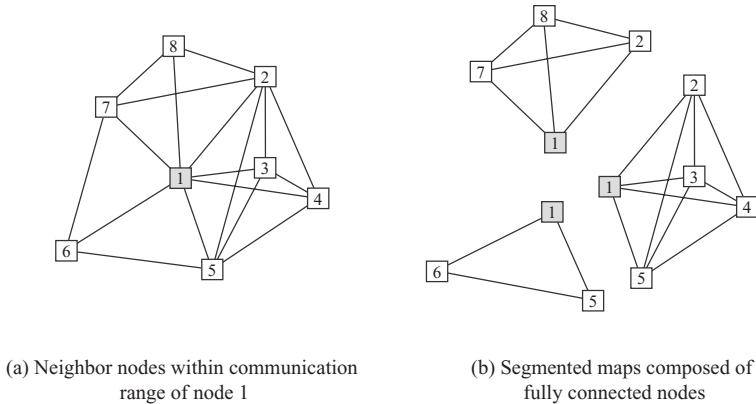


Fig. 1. Node deployed example within communication range of node 1: (a) real deployment of node 1 and its neighbor nodes, (b) segmented maps of node 1 of the LaMSM

node 6, so that it cannot measure the distance to node 6. In this case, MDS-MAP(P) calculates the distance as $d_{26} = \min(d_{21} + d_{16}, d_{27} + d_{76}, d_{25} + d_{56})$: whatever it selects is an indirect distance for the real distance between node 2 and node 6.

3.2 LaMSM: Localization Algorithm with Merging Segmented Maps

In the proposed LaMSM, a segmented map is newly defined as a basic unit to make a reliable local map. LaMSM is composed of two phases: building a local map with segmented maps at every node and constructing a global map with collected local maps at a special node.

A. Building Segmented Maps from Measured Distances. Each node measures distances from itself to neighbor nodes by resolving delays at received acoustic packets, and then sends and receives the distance information to neighbor nodes. Then, each node realizes most distances between neighbor nodes but still has some unmeasured distances between them. To avoid calculating the unmeasured distance, it segments measured distances into sub-distance sets. Elements in a sub-distance set are distances between nodes which are fully connected to one another, so that there is no unmeasured distance in a sub-distance set. Applying MDS to each sub-distance set, each node can immediately build a few segmented maps which are the basic units to construct a local map. For instance, node 1 can build three segmented maps with sub-distance sets, as shown in Fig. 1(b). All nodes in each segmented map are connected to one another, so that they can measure all distances between them. Hence, node 1 does not need to calculate any unmeasured distance like d_{26} to build segmented maps but it is necessary to merge three segmented maps together for a local map in Fig. 1(a).

B. Merging Segmented Maps for a Local Map. Once segmented maps are secured, the next work of each node is to merge them for a local map. Each node selects a segmented map which has the most nodes among the segmented maps, as a reference map. The other segmented maps are merged into the reference map sequentially by relocating them on the coordinates of the reference map. A merging order is determined with the number of common nodes between a reference map and the other segmented maps. Hence, it is important to minimize errors arising in every merging time, otherwise errors continuously increase at the next merging time.

Let's consider two maps: a reference map and a segmented map, which have m common nodes in the p -dimensional Euclidean space, usually $p = 2$ or 3 . The position matrices for m common nodes are represented as $\mathbf{A} = [\mathbf{a}_j]_{p \times m}$ in a segmented map and $\mathbf{B} = [\mathbf{b}_j]_{p \times m}$ in a reference map, respectively. While merging the segmented map to a reference map, each node computes three parameters: a scaling parameter s , an orthonormal rotating (optionally reflecting) matrix \mathbf{R} , and a translating vector \mathbf{t} , in order to minimize the following discrepancy error $E(s, \mathbf{R}, \mathbf{t})$ between two common node sets:

$$E(s, \mathbf{R}, \mathbf{t})^2 = \sum_{j=1}^m \|s\mathbf{R}\mathbf{a}_j + \mathbf{t} - \mathbf{b}_j\|^2 . \tag{1}$$

For the parameters, we adopt Umeyama's method [10] which determines the rotating matrix \mathbf{R} with the singular value decomposition. According to Umeyama's method, three parameters can be expressed as

$$\begin{aligned} \mathbf{R} &= \mathbf{U}\mathbf{S}\mathbf{V}^T , \\ s &= \frac{\text{trace}(\mathbf{D}\mathbf{S})}{\frac{1}{m} \sum_{j=1}^m \|\mathbf{a}_j - \bar{\mathbf{a}}\|^2} , \\ \mathbf{t} &= \bar{\mathbf{b}} - s\mathbf{R}\bar{\mathbf{a}} , \end{aligned} \tag{2}$$

where $\bar{\mathbf{a}} = \frac{1}{m} \sum_{j=1}^m \mathbf{a}_j$, $\bar{\mathbf{b}} = \frac{1}{m} \sum_{j=1}^m \mathbf{b}_j$, $\mathbb{A} = [\mathbf{a}_j - \bar{\mathbf{a}}]_{p \times m}$, $\mathbb{B} = [\mathbf{b}_j - \bar{\mathbf{b}}]_{p \times m}$, $\mathbf{U}\mathbf{D}\mathbf{V}^T = \text{svd}(\mathbb{B}\mathbb{A}^T)$, and

$$\mathbf{S} = \begin{cases} \mathbf{I} & \text{if } \det(\mathbb{B}\mathbb{A}^T) \geq 0 \\ \text{diag}(1, 1, \dots, 1, -1) & \text{if } \det(\mathbb{B}\mathbb{A}^T) < 0 . \end{cases} \tag{3}$$

While merging two segmented maps, we do not use the scaling parameter in Eq. 2 to preserve the scale of all segmented maps as well as a reference map.

Because some segmented maps are given as being reflected in the coordinates of a reference map, rotating matrix \mathbf{R} needs to determine whether it reflects a segmented map or not, as well as to rotate it. However, Umeyama's method does not provide such a determination to reflect in the rotating matrix \mathbf{R} . Furthermore, it is hard to determine reflection of a segmented map only with common nodes when there are outliers in common nodes or when common nodes are almost placed on a straight line.

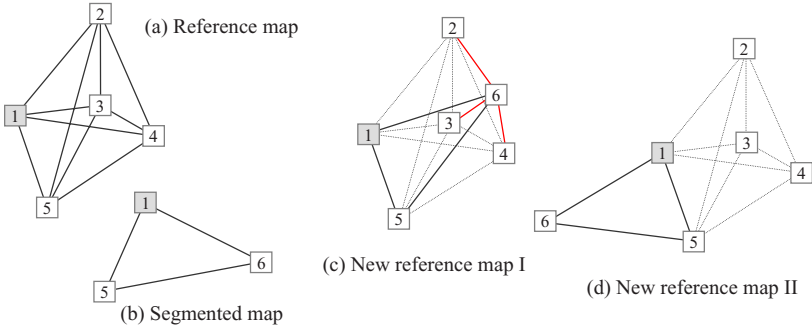


Fig. 2. Merging segmented maps for a local map: (a) reference map at node 1, (b) segmented map overlapped with a reference map at node 1, (c) new reference map I after merging an original segmented map, (d) new reference map II after merging a reflected segmented map

To determine reflection of a segmented map, LaMSM considers two kinds of segmented maps: an original segmented map and a reflected segmented map. LaMSM relocates two segmented maps on the coordinates of a reference map with three parameters in Eq. 2, respectively. Then, LaMSM can obtain independently two new reference maps for a segmented map. It then selects a new reference map that has less direct connections between excluded nodes. The excluded nodes mean the other nodes which remain in a segmented map and a reference map except common nodes. Because excluded nodes in a segmented map are placed out of the communication range of excluded nodes in a reference map, they do not have any direct connection to each other.

For example, a reference map and a segmented map are shown in Fig. 2(a) and 2(b). Their common nodes are nodes 1 and 5, excluded nodes of a reference map are nodes 2, 3, and 4, and an excluded node of a segmented map is node 6. With original and reflected segmented maps, two new reference maps are obtained: one is the new reference map I after merging an original segmented map, and the other is the new reference map II after merging a reflected segmented map, as shown in Fig. 2(c) and 2(d). While excluded node 6 of a segmented map has connections to excluded nodes 2, 3, and 4 in Fig. 2(c), it has no connections to any excluded nodes in Fig. 2(d). Hence, we can properly relocate a segmented map on the coordinates of the reference map by selecting the new reference map II, as shown in Fig. 2(d).

C. Merging All Local Maps for a Global Map. After building a local map by merging segmented maps, each node sends the local map information to a powerful node, such as a monitoring center, a sink node or a base station. Among the collected local maps, the powerful node selects the local map which has the largest number of nodes, as a reference map for a global map. Then, the other local maps are merged into the reference map with the same mechanism as the one used to merge segmented maps. The reference map becomes a global map

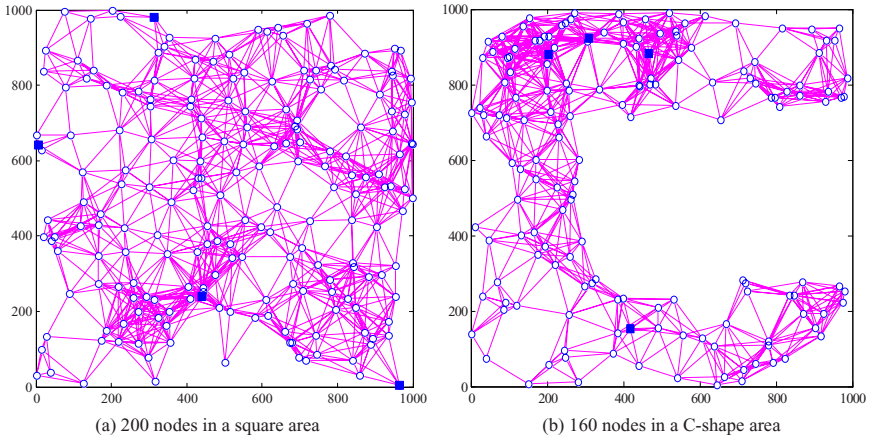


Fig. 3. Real deployments with 4 beacons marked as black square nodes: (a) 200 nodes in a square area, (b) 160 nodes in a C-shape area

after merging all local maps. Then, the powerful node relocates the global map with the given beacon nodes in order to assign all nodes the absolute positions, which can be achieved with Umeyama's method by regarding the given beacon nodes as common nodes of a real map. Here, the scaling parameter in Eq. 2 is used because the global map could be scaled up or down compared to a real map. Finally, we can get a global map where all nodes have their absolute positions. The main advantages of such a centralized algorithm using a powerful node are to alleviate network burden because it is not necessary to forward absolute positions to all nodes, and to improve accuracy in nodes' position using the global information of sensor nodes.

4 Simulation Results

To evaluate the proposed localization algorithm with merging segmented maps (LaMSM), we consider two distinct placements of nodes, as shown in Fig. 3: one is a regular placement where 200 nodes are randomly deployed over a 1000m \times 1000m square area, and the other is an irregular placement where 160 nodes are randomly distributed over a C-shape area, where dark square nodes are beacons which are supposed to be attached to buoys. Also, we assume that communication between nodes is possible within acoustic transmission range, $R = 150\text{m}$. The measured distance between nodes i and j contains a range error, which is modeled as $d_{ij} = v_a(t_{ij} + t_\epsilon) = d_{ij}^* + v_a t_\epsilon$ where $v_a = 1.5 \times 10^3\text{m/s}$ is the speed of sound underwater, d_{ij}^* is the real distance between nodes i and j , t_{ij} is actual time for d_{ij}^* , and t_ϵ is a range error which is a random value with the Gaussian distribution $N(0, \sigma^2)$. We ran the simulation 100 times to get the results under a different range error each time. To indicate average position error

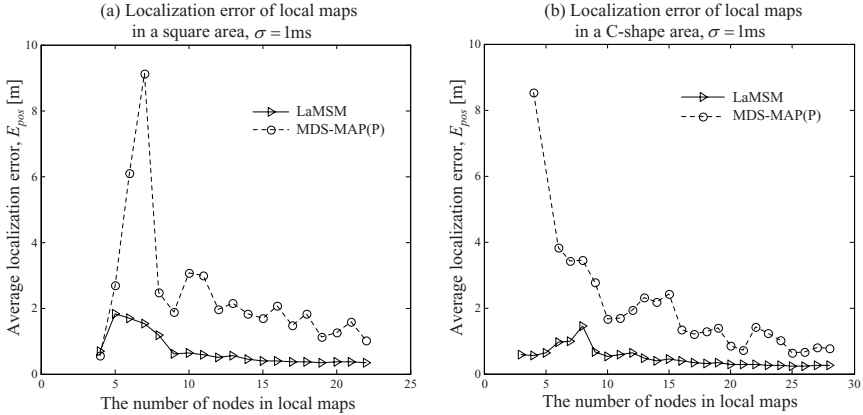


Fig. 4. Localization error in local maps built with LaMSM and MDS-MAP(P) under $\sigma = 1\text{ms}$ in (a) a square area and (b) a C-shape area, respectively

between positions of a real node and its estimated node, the average localization error of a node is defined as

$$E_{pos} = \frac{1}{n} \sum_{i=1}^n \|x_i^* - x_i\|, \tag{4}$$

where n is the number of nodes, x_i^* and x_i are the real position and the estimated position for a node i , respectively.

First, we compare the average localization error in local maps built with LaMSM and MDS-MAP(P). The number of nodes in a local map depends on node density. The average number of nodes in a local map is 12.3 in a square area and 12.5 in a C-shape area. The simulations of Fig. 4 were carried out under 1ms range error in time of flight (ToF). As shown in Fig. 4, local maps of LaMSM have lower and more regular localization error than those of MDS-MAP(P) because LaMSM never uses unmeasured distances which MDS-MAP(P) does. The average localization error of all local maps in LaMSM is 0.63m in a square area and 0.61m in a C-shape area, while it is 2.26m and 2.12m in MDS-MAP(P), respectively. Additionally, localization error of MDS-MAP(P) gradually declines with the increasing number of nodes in a local map; that is, the number of measured distances relatively increases rather than the number of the calculated distances with increasing node number, so that the effect of errors in the calculated distance is reduced correspondingly.

Fig. 5 shows the average localization error in a global map by varying the standard deviation of a range error from 0.2ms to 2ms. Results show that the accuracy of LaMSM is about 7.8 times better than MDS-MAP(P) in a square area and about 10.4 times better in a C-shape area at 0.2ms range error, as shown in Fig. 5(a) and 5(b), respectively. Even at 2ms range error, the accuracy of LaMSM is still better than MDS-MAP(P); that is, about 1.6 times in

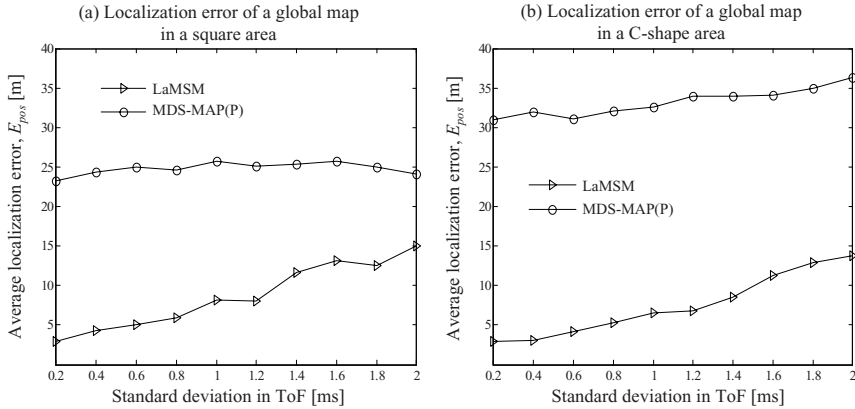


Fig. 5. Average localization errors for all nodes estimated with LaMSM and MDS-MAP(P) in (a) a square area and (b) a C-shape area

a square area and 2.6 times in a C-shape area. Overall, the cause of relatively high localization error in MDS-MAP(P) is that errors arising from calculating unmeasured distances are dominant over range errors when it constructs local maps. Furthermore, the performance of LaMSM is analogous in both node deployments, while MDS-MAP(P) performs better in a square area than a C-shape area.

5 Conclusions

We presented the localization algorithm with merging segmented maps (LaMSM) for underwater sensor networks (UWSNs). Underwater sensor nodes use acoustic signals to communicate due to its long transmission range, which makes it possible to measure accurately distances between nodes by resolving the delay of acoustic signals.

As a basic unit for a global map in LaMSM, a segmented map is composed of the only fully connected nodes; that is, the map is built with only the measured distances. Hence, it can avoid calculating unmeasured distances that result in errors in accuracy. In fact, LaMSM has about 3.5 times better accuracy in a local map than the well-known MDS-MAP(P). Furthermore, LaMSM provides a closed-form solution to minimize localization errors arising from merging maps, where it utilizes node connections to correctly decide whether a map is reflected or not. According to our simulation results, LaMSM outperforms MDS-MAP(P) with respect to localization accuracy: at least 1.6 times in a square area, and 2.6 times in a C-shape area, even at 2ms range error.

Accurate position information is useful to various ocean applications, such as exploring geographical features, developing natural resources underwater, protecting from ocean disasters, etc. To secure accurate position information, more

elaboration is required in resolving the delay of time of flight (ToF), time synchronization, and localization algorithms. In the future our work will be to investigate LaMSM under realistic environment, three-dimensional Euclidean space.

Acknowledgment

This work was supported by the Center for Distributed Sensor Network at GIST.

References

1. Akyildiz, I.F., Pompili, D., Melodia, T.: Underwater Acoustic Sensor Networks: Research Challenges. *Ad Hoc Networks Journal* , 257–279 (2005)
2. Cui, J., Kong, J., Gerla, M., Zhou, S.: The Challenges of Building Scalable Mobile Underwater Wireless Sensor Networks for Aquatic Applications. *IEEE Networks Mag.* , 12–18 (2006)
3. Oh, M., Raftery, A.: Bayesian Multidimensional Scaling and Choice of Dimension. *Journal of the American Statistical Association* 96(455), 1031–1044 (2001)
4. Shang, Y., Ruml, W., Zhang, Y., Fromherz, M.: Localization from Mere Connectivity. In: *Proc. of the 4th ACM Intr. Symp. on Mobile and Ad-Hoc Networking & Computing*, pp. 201–212 (2003)
5. Shang, Y., Ruml, W.: Improved MDS-Based Localization. *Proc. of IEEE INFOCOM 4*, 2640–2651 (2004)
6. Shang, Y., Ruml, W., Zhang, Y., Fromherz, M.: Localization from Connectivity in Sensor Networks. *IEEE Trans. Parallel and Distributed Systems* 15(11), 961–974 (2004)
7. Moore, D., Leonard, J., Rus, D., Teller, S.: Robust Distributed Network Localization with Noisy Range Measurements. In: *Proc. of ACM SenSys 2004*, pp. 50–61 (2004)
8. Kwon, O., Song, H.: A New Map Stitching Method for Anchor-free Localization in Wireless Sensor Networks. In: *IEEE Conf. on Computer and Information Technology*, pp. 236–236 (2006)
9. Horn, B.K.P., Hilden, H.M., Negahdaripour, S.: Closed-form Solution of Absolute Orientation Using Orthonormal Matrices. *Journal of the Optical Society of America A* 5(7), 1127–1135 (1988)
10. Umeyama, S.: Least-Squares Estimation of Transformation Parameters between Two Point Patterns. *IEEE Trans. Pattern Analysis and Machine Intelligence* 13(4), 376–380 (1991)

TinyOS-Based Gateway for Underwater Acoustics/Radio Frequency Communication

Phil-Jung Yun, Changhwa Kim, Sangkyung Kim,
Seung-Jae Lee, and Yong-Man Cho

Department of Computer Science & Engineering,
Kangnung National University

Gangneung Daehangno 120, Gangneung-Si, Gangwon-Do, 210-702, Korea
Tel.: +82-33-640-2897; Fax: +82-33-640-2899

`mars@cs.kangnung.ac.kr`, `{kch, skkim98, silveree, ymcho}@kangnung.ac.kr`

Abstract. Currently, UWASN (Underwater Acoustic Sensor Network) has been researched as a branch of sensor networks. UWASNs use a transmission media different from terrestrial wireless sensor networks. That is, the former uses acoustic waves and the latter uses radio waves for communication. G/W (Gateways) in UWASNs are nodes for relaying data transmission between a UWASN and a terrestrial wireless sensor network. So, it is necessary to design and realize the UWA communication module with the UWA/RF (Underwater Acoustics/Radio Frequency) protocol stack for the underwater environment. As TinyOS used most widely at operating system for sensor networks is not considering the underwater acoustic communication, the functions supported by it cannot be used. Therefore, The TinyOS-based UWA/RF G/W system and prototype suitable for the characteristic of UWASN is designed and realized in this paper.

Keywords: Underwater Acoustic Sensor Network, Underwater Acoustics/Radio Frequency, Gateway, TinyOS.

1 Introduction

As acoustic waves are attenuated faster than radio waves in the air and vice versa in the underwater, it is needed to use more proper method for communication in each environment. Currently, for radio wave communication in the underwater, very low frequency (30-300Hz), very long antennae and very high transmission power are needed. Although optical waves are used, it suddenly diminishes in the underwater. Therefore, acoustic waves are used for underwater communication [1].

Acoustic waves have very different characteristics from radio waves in speed, bandwidth and transmission energy [2], [3], [4], [5]. It has slower speed, narrower bandwidth and fewer channels than radio waves [6], [7], [8]. It also needs more transmission power than radio wave [9].

Underwater acoustic communication has many different characteristics and these are listed below

- **Communication Range:** As low frequency waves are used in UWASN, it has longer communication range than radio waves.
- **Communication Power:** Acoustic communication needs more transmission energy.
- **Channel:** There are only a few channels available in acoustic communication. Communication speed is very slow, variable and multi-path and fading problems might happen.
- **Bandwidth:** It has very low bandwidth.
- **Cost:** The costs of sensor nodes and acoustic modems are high.
- **Deployment:** The density of sensor nodes affects the cost and the communication range. Multi-hop communication is more effective than direct communication in transmission energy if the distance between two nodes is long [10]. A sparse UWASN increases the communication cost and a dense UWASN increases the communication cost. Therefore, density of a UWASN should be determined by application objectiveness of the UWASN.
- **Energy Limit:** Energy of UWASNs is very limited because it is very hard to recharge the batteries.
- **High Error Rate:** The bit error rate in acoustic communication is high.

UWASNs have been studied with the focusing on network and MAC layer for considering the characteristics of UWASNs and acoustic modems for UWA communication. Ethem M. Sozer and Milica Stojanovic has developed Reconfigurable Acoustic Modem (rModem) [11], [12] and Jack Wills, Wei Ye and John Heidemann have developed Low-Power Acoustic Modem for Dense deployment for UWASN [13].

However, although it is necessary to send queries from terrestrial centers to UWASN sensor nodes and to send data from UWASN sensor nodes to terrestrial centers, the researches for relaying data transmission between UWASNs and the ground network are very rare. We have tried to study and implement UWA/RF G/W system before developing UWA/CDMA or UWA/satellite G/W system.

The objective of the UWA/RF G/W system is relaying data transmission between a UWASN and a terrestrial center. Sensed data in sensor nodes are transferred to a UWA/RF G/W via UWA communication and the data received by the acoustic modems of sensor nodes are transferred from the UWA/RF G/W to a terrestrial center via RF communication. The UWA/RF G/W system is positioned at the relay point and it must be designed and realized with consideration for both air and underwater environment because it uses both radio waves and acoustic waves. Additionally, the acoustic modem for physical communication and the protocol stack for effective communication is also needed.

Selection of the operating system is very important in developing the UWA/RF G/W system. It affects design, realization method, effectiveness and stability of the system. Therefore, the UWA/RF G/W is developed in this paper based on TinyOS 2.0.0 Beta which has much strength for sensor networks.

The rest of this paper is constructed as follows. In section 2, requirements for UWA/RF G/W are presented and section 3 illustrates UWA/RF sensor network

system environment. Section 4 shows the UWA/RF G/W system design and section 5 describes the UWA/RF G/W system prototype. Finally, section 6 concludes and finalizes this paper.

2 Requirements for UWA/RF G/W System

The requirements for design and realization of the UWA/RF G/W system are divided into four categories as follows:

First, the acoustic modem and UWA communication module considering the underwater must be realized because underwater sensor nodes communicate each other using acoustic waves.

Second, the UWA/RF G/W protocol stack considering underwater environment and UWASN characteristics should be designed. Because the sensor network standard specifications currently used, i.e. IEEE 802.15.4 and Zigbee, are not designed for underwater environment and UWASN characteristics.

Third, the management functions for communication modules must be analyzed and realized because UWA/RF G/W nodes communicate using both radio waves and acoustic waves.

Finally, a proper operation system be selected considering stability, reconfiguration cost, etc.. TinyOS used in this paper is a component-based operation system for sensor networks and supports reusability, compatibility, portability and productivity.

3 UWA/RF Sensor Network Architecture

Fig. 1 shows the UWA/RF sensor network architecture. It transfers sensed data to terrestrial centers and transfers queries to sensor nodes. And it consists of UWA sensor nodes, UWA/RF G/W nodes and RF relay nodes.

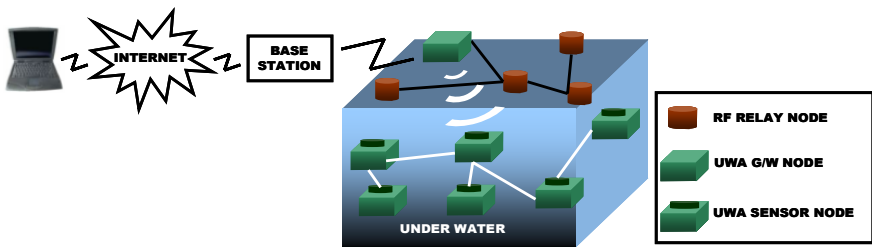


Fig. 1. UWA/RF Sensor Network Architecture

UWA sensor nodes sense underwater environment and communicate with other UWA sensor nodes. UWA/RF G/W nodes convert radio waves to acoustic waves and vice versa. And RF relay nodes relay UWA/RF G/W nodes and terrestrial centers when a UWA/RF G/W cannot communicate directly with a terrestrial center.

4 Design of TinyOS-Based UWA/RF G/W Design

The protocol stack of the UWA/RF G/W and the UWA/RF G/W system are designed in this section. Fig. 2 shows the protocol stack of the UWA/RF G/W and it consists of Gateway Module, Communication Module Transmission Manager, UWA MAC layer, UWA PHY layer and Communication Module Reception Manager.

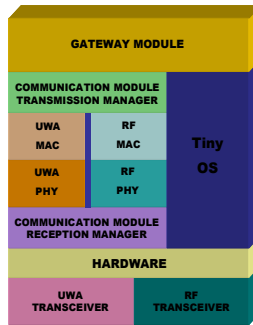


Fig. 2. UWA/RF G/W Protocol Stack

Gateway Module supports the functions that control and manage the UWA/RF G/W node. Communication Module Transmission Manager solves the problems that might occur during multiple instances of Communication Module being executed. The UWA MAC layer provides MAC functions which are proper to underwater environment. The UWA PHY layer controls and manages hardware, ensures link quality and selects channels. Communication Module Reception Manager prevents problems which might occur during reception with multiple instances of Communication Module.

4.1 Gateway Module

Gateway Module is designed like Fig. 3 and the ITRC_GATEWAYMODULE component provides functions that enable to control the UWA/RF G/W node according to the event that occurs in the UWA/RF G/W node. The events are reception completion events of messages for RF or for UWA.

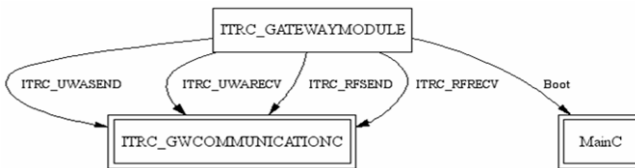


Fig. 3. Gateway Module Design

The event caused by reception completion event for RF message occurs when a query sent to sensor nodes arrives and the reception completion event for UWASN message occurs when a response of a query or a sensed data sent to a terrestrial center arrives.

4.2 Communication Module Transmission Manager

Fig. 4 shows Communication Module Transmission Manager and consists of ITRC_GWCOMMUNICATIONP and ITRC_TRANSMISSIONMANAGERP components.

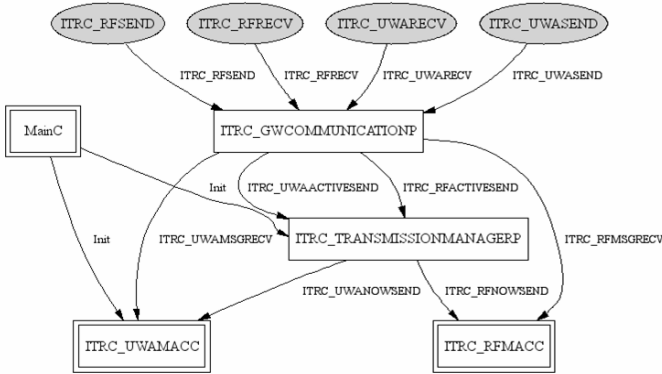


Fig. 4. Design of Communication Module Transmission Manager

ITRC_GWCOMMUNICATIONP transfers a request or an event to each component after it determines whether it is a transmission request to RF, UWA communication module or an event for reception completion.

ITRC_GWCOMMUNICATIONMANAGER serializes the transmission requests from RF and UWA and it enables to be processed in turn. The scheduler of TinyOS also supports multiple transmission requests [14]. If current transmission message is a request to the RF communication module, the request is delivered to ITRC_RFMACC. Or if it is a request to the UWA communication module, it is delivered to ITRC_UWAMACC.

Table 1. Interface supported by Communication Module Transmission Manager

| Interface | Functions |
|--------------------|--|
| ITRC_UWASEND | Processing transmission message for reporting transmission completion for UWA messages |
| ITRC_RFSEND | Processing transmission message for reporting transmission completion RF messages |
| ITRC_UWARECV | Reporting reception completion of UMA messages and delivering received messages |
| ITRC_RFRECV | Reporting reception completion of RF messages and delivering received messages |
| ITRC_UWAACTIVESEND | Scheduling UWA transmission requests with serialization |
| ITRC_RFACTIVESEND | Scheduling RF transmission requests with serialization |

The interfaces that Communication Module Transmission Manager supports are listed in Table 1.

4.3 UWA MAC Layer

Fig. 5 shows the design of the UWA MAC layer. It consists of ITRC_UWAMACP and ITRC_UWACHANNELACCESSP components.

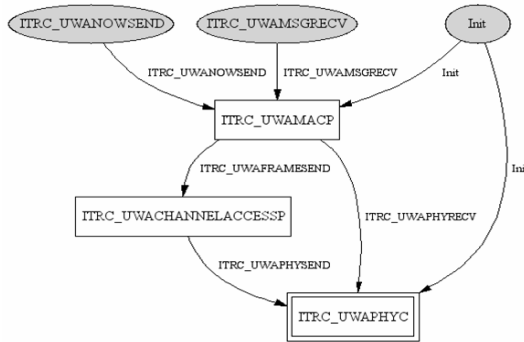


Fig. 5. Design of UWA MAC Layer

ITRC_UWAMACP frames messages received with transmission request from Communication Module Transmission Manager. The frames include a sequence number, CRC and frame size. On receipt of a frame, it delivers received frames to the next higher layer after error check.

ITRC_UWACHANNELACCESSP determines the channel access method for transmitting a frame generated at ITRC_UWAMACP and transmits the frame by the method.

Table 2. Interfaces provided by the UWA MAC layer

| Interface | Functions |
|-----------------------|---|
| ITRC_UWANOWS END | Converting messages to frames |
| ITRC_UWAFRAM ESEND | Processing the transmission request for UWA frame with defined channel access method by the system. Reporting transmission completion |
| ITRC_UWAMSGR ECV | Reporting reception of UWA frame. Delivering the payload after checking errors of a received UWA frame |

Table 2 shows the list interfaces which the UWA MAC layer provides in order to process transmission request from Communication Module Transmission Manager.

4.4 UWA PHY Layer and Communication Module Reception Manager

The UWA PHY layer and Communication Module Reception Manager are designed like Fig. 6. The UWA PHY layer consists of the ITRC_UWAPHYP component and Communication Module Reception Manager consists of the ITRC_UWARECEPTIONMANAGERP component.

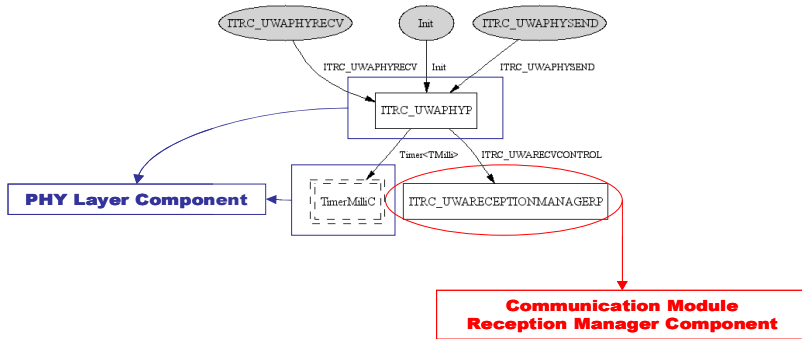


Fig. 6. Design of UWA PHY Layer and Communication Module Reception Manager

ITRC_UWAPHYP transfers frames through the acoustic modem after transforming it to PDU-1(Protocol Data Unit-1) given a transmission request from the UWA MAC layer. If there is a received PDU-1, it delivers a received PDU-1 with the report that it receives PDU-1 from the UWA MAC layer.

On receiving a frame from the acoustic modem, ITRC_UWARECEPTIONMANAGERP resolves problems that might occur by multiple instances of Communication Module Reception Manager by disabling the reception interrupt from all of instances of Communication Module Reception Manager except the acoustic modem during receiving a frame.

Table 3. Interfaces supported by UWA PHY Layer and Communication Module Reception Manager

| Interface | Functions |
|---------------------|---|
| ITRC_UWAPHYSEND | Transmitting transmission requests for a UWA frame with the acoustic modem. Reporting transmission completion |
| ITRC_UWAPHYRECV | Reporting reception of PDU-1. Delivering the received PDU-1 |
| ITRC_UWARECVCONTROL | Disabling interrupts from other communication modules after detecting reception at the UWA PHY layer. |

The interfaces supported by the UWA PHY layer and Communication Module Reception Manager are listed in Table 3. The interfaces supported by the UWA PHY layer processes transmission requests from the UWA MAC layer.

5 Implementation of TinyOS-Based UWA/RF G/W Prototype

UWA/RF G/W prototype based on TinyOS using a UWASN acoustic modem which can be used at UWASN nodes is realized in this section.

5.1 Overview of the Acoustic Modem

The characteristics of the acoustic modem used in this research are as follows.

- Operating Voltage: 3.3V
- Frequency: 40 KHz(ultra sonic wave)
- Modulation Method: Amplitude Shift Keying
- Communication Mode: Uni-directional
- Data rate: 100bps.

5.2 The Algorithm for Gateway Module

The pseudo-code for Gateway Module is shown in Fig. 7. The ITRC_RFRECV event means completion of receiving a RF message. If this event occurs, the received RF message is delivered to Gateway Module as a parameter. In the case that a received RF message means a query, this message is delivered to UWASN nodes through UWA Communication Module in UWA/RF G/W. Transmission request is delivered to Communication Module Transmission Manager using ITRC_UWASEND.

```

async event void ITRC_RFRECV(uint8_t* MESSAGE) {
    Transmission request of a UWA message with ITRC_UWASEND;
}
async event void ITRC_UWARECV(uint8_t* MESSAGE) {
    Transmission request of a RF message with TRC_RFSEND;
}

```

Fig. 7. The Pseudo-code for Gateway Module

```

task void RFSEND() {
    atomic { Transmission request for a RF message with ITRC_RFNOWSEND; }
}
task void UWASEND() {
    atomic {
        Transmission request for a UWA message with ITRC_UWANOWSEND; }
}
async command void ITRC_UWAACTIVESEND.SEND(uint8_t* MESSAGE) {
    atomic { Posting the UWASEND() task; }
}
async command void ITRC_RFACTIVESEND.SEND(uint8_t* MESSAGE) {
    atomic { Posting the RFSEND() task; }
}

```

Fig. 8. The Pseudo-code for Gateway Module

The ITRC_UWARECV event means completion of receiving a UWA message. If this event occurs, the received UWA message is delivered to Gateway Module as a

parameter. In the case that a received RF message means a response or sensed data from a UWA sensor node, this message is delivered to a terrestrial center through RF Communication Module in UWA/RF G/W. Transmission request is delivered to Communication Module Transmission Manager using `ITRC_RFSEND`.

The pseudo-code for Communication Module Transmission Manager is presented in Fig. 8. `ITRC_UWAACTIVESEND.SEND()` is called by transmission request for a UWA message at Gateway Module and `ITRC_RFACTIVESEND.SEND()` is called by transmission request for a RF message at Gateway Module. Because all the requests are serialized by the scheduler in TinyOS, a task with processing parts of a function is posted on the scheduler when a transmission request occurs.

```
typedef nx_struct UWAFRAME {
    nx_uint8_t SEQ : 3;
    nx_uint8_t PAYLOAD[9];
    nx_uint8_t CRC : 5;
} UWAFRAME;
```

Fig. 9. UWA Frame Structure

Fig. 9 shows the frame structure of UWA frames. This frame consists of 3 bits sequence number, 5 bits CRC and 9 bytes payload.

```
async command void ITRC_UWANOWSEND.SEND(uint8_t* MESSAGE) {
    Inserting the message into payload of the UWAFRAME structure;
    Inserting the sequence number into payload of the UWAFRAME structure;
    if(SEQUENCE NUMBER == 7) {SEQUENCE NUMBER = 1;}
    else { SEQUENCE NUMBER++; }
    Calculating a CRC-5 value of the UWAFRAME structure;
    Inserting the CRC-5 value into payload of the UWAFRAME structure;
    Transmission request for the UWA frame with ITRC_UWAFRAMESEND;
}
```

Fig. 10. The Pseudo-code for transmission in the UWA MAC layer

The pseudo-code for transmission in the UWA MAC layer is like Fig. 10. When `ITRC_UWAPHYSEND.SEND()` is called by transmission request from Communication Module Transmission Manager, this function receives a UWA frame in the parameter. `ITRC_UWANOWSEND.SEND()` frames the received UWA message. Then, it inserts the message into payload of the frame and assigns the sequence number with `SEQ`. Calculated CRC value are also inserted into the frame. Finally, generated frame and transmission request are delivered to the UWA PHY layer.

The pseudo-code for the UWA PHY layer is described in Fig. 11. When `ITRC_UWAPHYSEND.SEND()` is called by transmission request from the UWA MAC layer, this function receives a UWA frame in the parameter. If the state of the acoustic modem is not `IDLE`, it discards the request because the acoustic modem is currently receiving some data. If not, it starts to transmit the frame. In this case, the state of the acoustic modem is set to `BUSY`, the timer is reset according to the

communication cycle of the acoustic modem and one by one bit at a time is transmitted as the timer is fired. After transmitting all the frame, the timer is stopped and the state of the acoustic modem is set to IDLE. Finally, it causes the

```

async command void ITRC_UWAPHYSEND.SEND(uint8_t* FRAME) {
  atomic {
    if(Acoustic Modem STATE!= IDLE) {}
    else {
      Disabling interrupts of the acoustic modem;
      Acoustic Modem STATE = BUSY;
      call MilliTimer.startPeriodic(Transmission cycle);
    }
  }
}
event void MilliTimer.fired() {
  atomic {
    if(Most significant bit of the frame == 1) {
      Generating transmission interrupt of the Acoustic Modem;
    }
    FRAME = FRAME << 1;
    if(end of the frame) {
      call MilliTimer.stop();
      Acoustic Modem STATE = IDLE;
      signal ITRC_UWAPHYSEND.SENDDONE();
    }
  }
}

```

Fig. 11. UWA PHY Send Algorithm

UWAPHYSEND.SENDDONE event so that reports transmission completion to the UWA MAC layer.

```

async command void ITRC_UWARECVCONTROL.ROCK() {
  atomic {
    Disabling reception interrupt of CC2420;
    Enabling reception interrupt of the acoustic modem;
  }
}
async command void ITRC_UWARECVCONTROL.UNROCK() {
  atomic {
    Enabling reception interrupt of CC2420;
  }
}

```

Fig. 12. Communication Module Reception Manager Algorithm

The pseudo-code for Communication Module Reception Manager is described in Fig. 12. On receiving the first bit of a frame at the acoustic modem, ITRC_UWARECVCONTROL.ROCK() is called. Reception completion report for

the first bit of a frame from the acoustic modem is a signal that it receives a bit of a frame and means that it starts receiving a frame. In this case, it disables reception interrupt from all other instances of Communication Module. On finishing reception task for a frame, ITRC_UWARECVCONTROL.UNROCK() is started. This function solves problems that might occur with multiple instances of Communication Module by enabling reception interrupt.

6 Conclusions and Future Works

In this paper, relaying method between UWASNs and terrestrial centers using UWA/RF G/W is proposed. UWA/RF G/W based on TinyOS is designed with consideration for the underwater and the characteristics of UWASN. The UWA/RF G/W protocol stack for effective communication in the UWA/RF G/W system is also designed and realized. In addition, Communication Module Transmission Manager and Communication Module Reception Manager are designed and realized to support managing multiple instances of Communication Module.

Effective Channel Access Methods and the network layer for the UWA/RF G/W system and design and realization of components for UWASN systems will be explored in the future.

Acknowledgments. This research was supported by the MIC (Ministry of Information and Communication), Korea, under the 2006 ITRC (Information Technology Research Center) contract number IITA-2006-C1090-0603-0044 support program supervised by the IITA(Institute of Information Technology Assessment).

References

1. Stojanovic, M.: Acoustic (underwater) Communications. In: Proakis, J.G. (ed.) Encyclopedia of Telecommunications, Wiley, New York (2003)
2. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A Survey on Sensor Networks. IEEE Communications Magazine (2002)
3. Proakis, J.G., Sozer, E.M., Rice, J.A., Stojanovic, M.: Shallow Water Acoustic Networks. IEEE Communications Magazine (2001)
4. Jurdak, R., Lopes, C.V., Baldi, P.: Battery Lifetime Estimation and Optimization for Underwater Sensor Networks. IEEE Press, New York (2004)
5. Sozer, E., Stojanovic, M., Proakis, J.: Underwater Acoustic Networks. IEEE Journal of Oceanic Engineering , 70–83 (2000)
6. Freitag, L., Stojanovic, M.: Acoustic Communications for Regional Undersea Observatories. In: Proceedings of Oceanology International, London, UK (2002)
7. Freitag, L., Stojanovic, M., Singh, S., Johnson, M.: Analysis of Channel Effects on Direct-sequence and Frequency-hopped Spread-spectrum Acoustic Communication. IEEE Journal of Oceanic Engineering , 586–593 (2001)
8. Stojanovic, M.: Recent Advances in High-Speed Underwater Acoustic Communications. IEEE Journal of Oceanic Engineering , 125–136 (1996)

9. Akyildiz, I.F., Pompili, D., Melodia, T.: State-of-the-Art in Protocol Research for Underwater Acoustic Sensor Networks. In: International Workshop on Underwater Network, MobiCom, pp. 7–16 (2006)
10. Pottie, G.J., Kaiser, W.J.: Embedding The Internet: Wireless Integrated Network Sensors. *Communications of the ACM*, 51–58 (2000)
11. Sozer, E.M., Stojanovic, M.: Time Synchronization for High Latency Acoustic Networks. In: Proceedings of the International Symposium on Unmanned Untethered Submersible Technology(UUST), Lee, New Hampshire, USA (2005)
12. Sozer, E.M., Stojanovic, M.: Reconfigurable Acoustic Modem for Underwater Sensor Networks. In: International Workshop on Underwater Network, MobiCom, pp. 101–104 (2006)
13. Wills, J., Ye, W., Heidemann, J.: Low-Power Acoustic Modem for Dense Underwater Sensor Networks. In: International Workshop on Underwater Network, MobiCom, pp. 79–85 (2006)
14. Levis, P., Sharp, C.: Schedulers and Tasks,
http://tinys.cvs.sourceforge.net/*checkout*/tinys/tinys-2.x/doc/html/tep106.html

An Energy Scheduling Algorithm for Ensuring the Pre-determined Lifetime in Sensor Network

Yong-Man Cho, Seung-Jae Lee, Changhwa Kim, and Sangkyung Kim

Department of Computer Science & Engineering, Kangnung National University
Gangneung Daehangno 120, Gangneung-Si, Gangwon-Do, 210-702, Korea
Tel.: +82-33-640-2897; Fax: +82-33-640-2899
{ymcho, silverree, kch, skkim98}@kangnung.ac.kr

Abstract. Energy limitation of a sensor network is a very important feature which distinguishes it from traditional networks and a number of methods to saving energy consumption have been studied in sensor networks. Most of those works have focused on Network, MAC or PHY layer and the lifetime of a sensor network cannot be pre-determined. But some sensor network might be able to survive for some specified time. In this work, we propose an energy consumption scheduling model, at application level of a node, that ensures pre-determined lifetime. To do this, first, we divide applications into six classes and define five operations of an application. Second, an energy consumption model is proposed using those five operations and consumption energies of each operation are calculated by a statistical method. Finally, energy consumption schedules of each application are rebuilt for a node to survive for pre-determined lifetime, e.g. varying the period of response and sensing and the number of actuation, etc. Consequently, it is ensured for nodes to survive for the pre-determined lifetime.

Keywords: energy scheduling algorithm, pre-determined lifetime, energy consumption model.

1 Introduction

Recently, the progress of wireless communication and computing technology has led the development of very small-sized sensor nodes. A sensor node is composed of sensors, which gather various environmental data, sensed-data processing unit, short-ranged wireless communication transceiver, and power unit [1]. A sensor network might be considered as a distributed computing platform that has the restricted processing power, small-sized memory, and the limited bandwidth and power.

More than anything else, a sensor node's limited energy provided by a battery requires a big effort to overcome in sensor networks. Many researches have been studied focusing on the methodologies and algorithms to consume a sensor node's energy efficiently. They include energy-efficient routing, data aggregation employing

clustering, energy-efficient MAC algorithm, data reporting period control, and so on. [2] and [3] proposed to extend the lifetime of a sensor network by minimizing energy consumption with cutting off a sensor node's transceiver while it is not participating in communications. These researches are related to enhancing energy efficiency in a MAC layer. Many researchers have studied energy-efficient routing algorithms. MMRE [5] selects a route toward the most energy-remained nodes after referring to each node's remained energy recorded in routing tables. MTE [6] selects a route consuming little energy by calculating the energy to transmit data to the next node. [7] and [8] combined the above two algorithms and suggested optimal routing algorithms. [9] and [10] control the network topology to operate minimum number of nodes within a network management area, alternately sleep nodes of which regions are overlapped to sense events, or minimize operating time by repeating sleep/wake based on each node's time table.

These researches are related to the methods to reduce the energy consumption at a whole network level and show quite good results at an entire sensor network system's perspective. While the existing researches have aimed at increasing the lifetime of a sensor network, our research intends to pre-determine the lifetime of a sensor network and make an energy consumption schedule to survive for the time. This energy consumption schedule is not a centralized, but an individual node based approach. This approach will prevent the generation of additional messages in a sensor network to mitigate the waste of energy.

The rest of this paper is as follows. Section 2 describes the basic strategy for energy consumption model. Section 3 explains our energy consumption model and scheduling algorithm. The last section remarks our conclusions.

2 Basic Strategy for Energy Consumption Model

To construct a energy consumption planning model, it needs the basic strategy like Fig. 1. We assume that the amount of consumption energy for an application is different from that of another application and we divide application types by

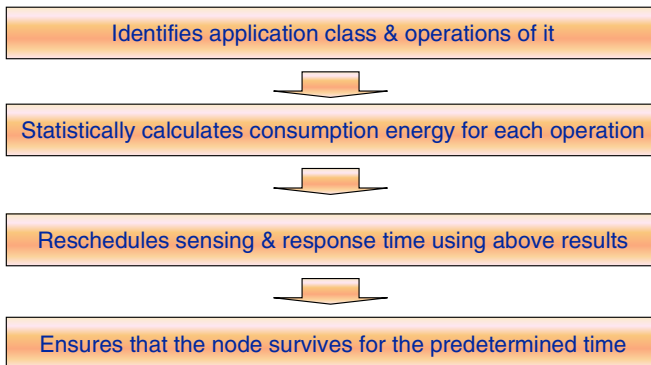


Fig. 1. Strategies for Energy Consumption Model

characteristic of its transmission cycle and sensing cycle. As applications execute, each application consumes different amount of energy and these states could be presented with some operations. We can calculate consumption energy for each application by the operations, we make each sensor node be active until pre-determined life time by changing the calculated cycle.

The structures of sensor network are divided into two categories such as uni-directional and bi-directional. In uni-directional structure, a control center cannot control sensor nodes and sensing and transmission cycle are set initially at sensor nodes. In contrast to this, in bi-directional structure, a control center can control sensor nodes and sensor nodes work with the command such as synchronization message, clustering message, routing message, data transfer message and query message.

A query (application) which is transmitted from a control center to a sensor node could be divided into 6 types by the transmission (response) cycle and the sensing cycle like below.

- Cyclic query(it does not have a pre-determined life time)
- Timed query(it does not have a transmission cycle)
- Event driven query(it has not a transmission cycle but a pre-determined life time)
- Instant query(it does not have both a transmission cycle and a life time)
- Cyclic and Timed query
- Timed event driven query

Energy consumption state variations of an application as time goes by are presented in Fig. 2.with the operations listed below.

- Transmission or Response: This operation is for sending sensed data from a sensor node to a sink node, a control center and a neighbor node on routing path. In this operation, the transmitter consumes most of energy and the processing cost for transferring a message to the network layer, the MAC layer and the PHY layer is included in this operation.
- Reception: This operation is for receiving a query at a node. In this operation, the receiver consumes most of energy and the processing cost for delivering a message to the application layer is included in this operation. This operation cannot be controlled by the node itself.
- Sensing: This operation is for transforming sensed data to information. In this operation, most of energy is consumed with sensing and delivering to a processing module. The processing cost including calibration is included in this operation.
- Processing: This operation is for processing energy consuming scheduling according to the type of applications.
- Actuation: This operation is for operating actuators. In this operation, most of energy is consumed by LEDs and motors.

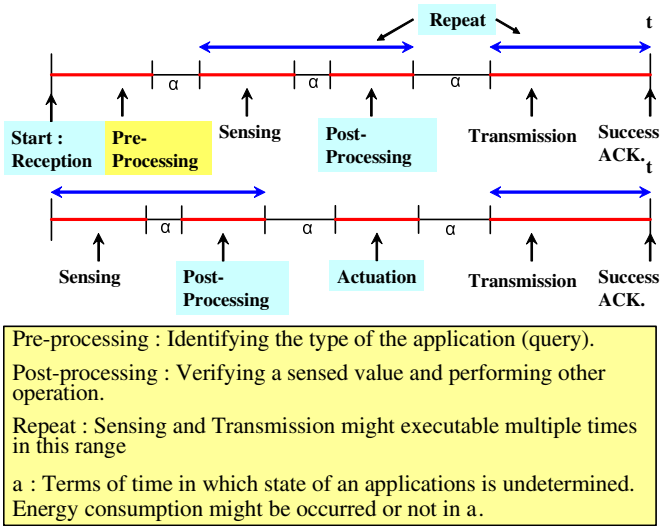


Fig. 2. The operation definitions for energy consumption state of a sensor node in which an application is running

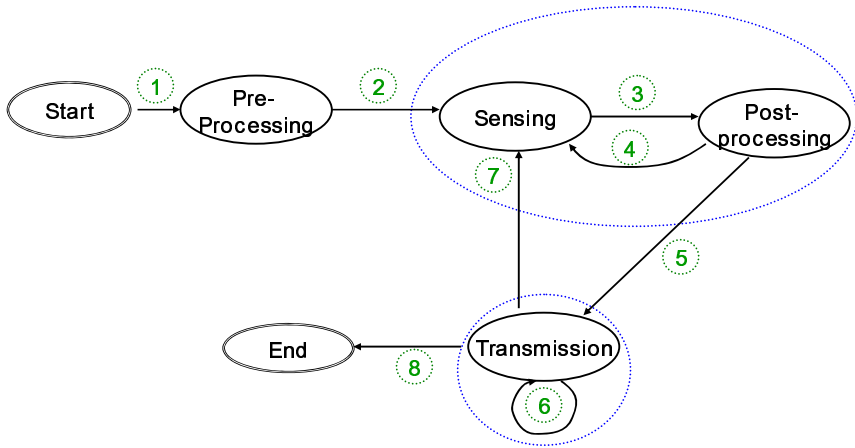


Fig. 3. State transition diagram of an application (STD: State Transition Diagram)

Fig. 3 shows the state transition diagram (STD) of an application, and explanations for each transition are like below.

- ① Prior to execute a query, it transits to Pre-processing state to analysis the type of a query.
- ② Transition to Sensing state with the type of a query.

- ③ Transition to Post-processing state with a sensed result.
- ④ According to the information at Pre-processing and Sensing, whether an event occurs or not it transits to Transmission state or Sensing state if it is an event driven query. And then, according the result whether there is an error or not, it transits to Sensing state or Transmission state.
- ⑥ Self-transition by transmission error.
- ⑦ Transition to Sensing state on valid query execution time.
- ⑧ Transition to End state on fired query execution time.

In Fig. 3, Actuation operation is not included. The reason is that most of sensor networks powers independently to actuators as it takes high energy.

Next, the energy model for determining consumed energy with the operations defined above is described.

3 Energy Consumption Model and Schedule Algorithm

An energy model is required to calculate the amount consumption energy of a node. We can express consumption energy as a function of time like (1).

$$E = E(t) \tag{1}$$

Among 5 operations defined previously, 3 operations except the transmission and sensing operations is uncontrollable. We call consumed energy by these three operations to. Therefore, we can express (1) as (2) which is a function of consumption energy of transmission and sensing.

$$E = E_{\beta} + n_T \times E_T + n_S \times E_S \tag{2}$$

n_T : the transmission count during time t.

n_S : the sensing count during time t.

To schedule these operations for surviving a pre-determined life time using (2), it needs (3), (4), (5) and (6).

$$N_{TS} = (E_{REM} - (T_{REM} \div T_{UNIT}) \times E_{\beta}) \div E_{TS} \tag{3}$$

$$T_{cycle} = T_{REM} \div N_{TS} \tag{4}$$

$$N_S = (E_{REM} - (T_{REM} \div T_{UNIT}) \times E_{\beta}) \div E_S \tag{5}$$

$$N_{cycle} = T_{REM} \div N_S \tag{6}$$

Table 1. Parameter used in functions

| Parameter | Description |
|-------------|---|
| E_{TS} | An estimated amount of consumption energy for a transmission. |
| E_S | An estimated amount of consumption energy for a sensing. |
| T_{REM} | Remained time for a sensor node to be survived in future. |
| T_{cycle} | Transmission cycle. |
| S_{cycle} | Sensing cycle. |
| NT_S | A maximum transmissible count for remained life time. |
| N_S | A maximum sensible count for remained life time. |

(3) is for that sensing cycle is dependent on transmission cycle and (5) is for that transmission cycle is dependent on sensing cycle. T_{cycle} and S_{cycle} mean how frequently sensing and transmitting for remained lifetime. Therefore, new transmission and sensing cycle for ensuring remained lifetime can be calculated. (3) and (5) can be reduced like below, where the unit of T_{REM} is equal to T_{UNIT}

$$N_{TS} = (E_{REM} - (T_{REM} \times E_{\beta})) \div E_{TS} \quad (7)$$

$$T_{cycle} = T_{REM} \div N_{TS} \quad (8)$$

$$N_S = (E_{REM} - (T_{REM} \times E_{\beta})) \div E_S \quad (9)$$

$$N_{cycle} = T_{REM} \div N_S \quad (10)$$

Energy consumption algorithm is for describing how to determine the counts of transmission and sensing operations for a sensor node to be survived during pre-determined life time. And this could be presented with 4 steps like below.

- Step 1: Identifying a received query.
- Step 2: Applying a proper energy consumption model to the query.
- Step 3: Executing the query by a calculated transmission cycle and sensing cycle.
- Step 4: Repeating step 2 and step 3 periodically until pre-determined life time.

4 Conclusion

In this paper, we propose an energy consumption scheduling algorithm in a sensor node with pre-determined life time, which is different from the other works. And we

classify application types in application layer, define the operations which consume energy and show that consumption energy by the operations can be calculated statistically. In addition, as the proposed algorithm forces that a sensor node survives for pre-determined life time, it also force that a whole sensor network survives for a given period.

Finally, research for enhancing the reliability of the algorithm proposed in this paper will be explored in the future.

Acknowledgement. This research was supported by the MIC (Ministry of Information and Communication), Korea, under the 2006 ITRC (Information Technology Research Center) contract number IITA-2006-C1090-0603-0044 support program supervised by the IITA (Institute of Information Technology Assessment).

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A Survey on Sensor Networks. *IEEE Communications Magazine* (2002)
2. Dam, T.V., Langendoen, K.: An adaptive energy-efficient MAC protocol for wireless sensor networks. In: *ACM SenSys 2003* (November 2003)
3. Deb, B., Bhatnagar, S., Nath, B.: A Topology Discovery Algorithm for Sensor Networks with Applications to Network Management. Technical Report DCS-TR-441, Department of Computer Science, Rutgers University (May 2001), (submitted for publication)
4. Chang, J.-H., Tassiulas, L.: Maximum lifetime routing in wireless sensor networks. In: Presented at the ATIRP Conf, College Park, MD (March 2000)
5. Gomez, J., Campbell, A.T., Naghshineh, M., Bisdikian, C.: Power-aware routing in wireless packet networks. In: *Mobile Multimedia Communication (MOMUC)*, San Diego (November 1999)
6. Xu, Y., Heidemann, J., Estrin, D.: Geography-informed Energy Conservation for Ad Hoc Routing. In: *Mobile Computing and Networking (MobiCom)*, Rome (July 2001)
7. Toh, C.K.: Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks. *IEEE communication magazine*, 138–147 (June 2001)
8. Ramanathan, R., Hain, R.: Topology control of multihop wireless networks using transmit power adjustment. *INFOCOM* (2000)
9. Kawadia, V., Kumar, P.R.: Power control and clustering in ad hoc networks. In *INFOCOM* (2003)

Underwater Acoustic Communication and Modem-Based Navigation Aids

Dale Green

Teledyne Benthos
49 Edgerton Drive
North Falmouth, MA 02556 USA

Abstract. New forms of navigation aids for underwater vehicles are enabled through the use of acoustic communications. Both the content and form of the message may be used to estimate range, bearing, range rate, geo-location, and time. Accurate range estimates are available via a conventional 2-way method, but the transmitted signal also supports high precision bearing estimation and highly accurate range rate compensation at the receiver. A new multi-access waveform supports asynchronous and simultaneous reception and processing of multiple messages leading to translation of conventional satellite GPS to the underwater environment. High accuracy tracking of underwater vehicles is enabled through a further modification of this multi-access signal. Recent advances in DSP-based, low-power modem development provide a rich infrastructure for accomplishing these navigation functions simultaneously with a variety of communications functions. Each of these developments are supported by recent at-sea experiments and demonstrations.

1 Introduction

In this paper we describe several practical navigation aids, each based upon our core acoustic communications technology. The technology is the result of numerous programs funded over the past ten years by the US Navy, as well as by substantial IR&D programs within Teledyne Benthos. The fundamental requirement for all of these inter-related efforts is the use of physically small, battery-powered, DSP-based hardware. The acoustic communications provides connectivity under most environmental conditions at data rates ranging from 80 bits per second (bps) to in excess of 10 Kbps. The navigation functions each involve novel developments in broadband acoustic signal processing. These include a broadband enhancement to an ultra-short baseline (USBL) bearing estimator, precision range estimation, precision estimation of and compensation for very high relative speed platforms (i.e., high range rate), translation of GPS to the underwater environment, and precision tracking of underwater vehicles. Each of these systems have been tested at sea with excellent results.

Section 2 describes some of the capabilities of the Telesonar modem, and highlights those signaling characteristics used to implement the navigation aids.

Section 3 describes three recently-developed navigation aids, along with results of recent at-sea experiments. Finally, Section 4 describes certain ongoing developments affecting both communications and navigation aids for undersea platforms.

2 Acoustic Signaling

The navigations aids described later in this paper use either of two non-coherent signaling schemes that are standard signaling formats in the Telesonar modem. The first is a frequency hopped, frequency shift keyed (FH/FSK) signal which is used either for extremely adverse channels or for multi-access situations. It is an inherently low data rate scheme, but one which tolerates a variety of linear and nonlinear processing designed to reduce the affects of interference and low SNR. In the Telesonar formulation, a pseudo-random hopping pattern, based upon finite field arithmetic, is used to position individual tonals (sinusoids) at discrete frequencies within a constrained bandwidth. Only one tonal is transmitted at one baud period. For the standard case of 6.25 ms tonals, combined with error correction coding, we transmit at approximately 80 bps. A typical operating bandwidth is 5120 Hz. Figure 1 shows a graphical formulation of a typical FH/FSK (binary) modulation.

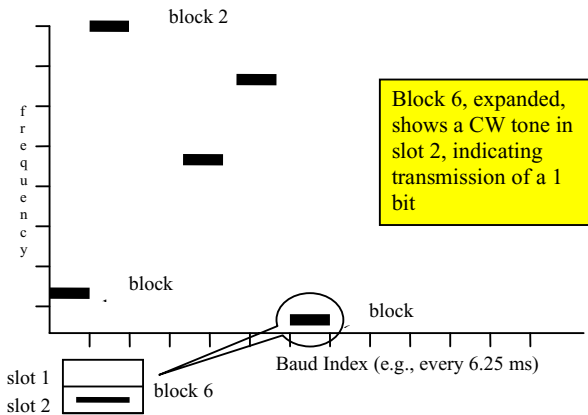


Fig. 1. Example of frequency-hopped binary FSK

The remarkable feature of the hopping patterns used here is that several signals can co-exist simultaneously within the same time- and frequency-space. The Telesonar modem is able to acquire and process four such signals at the same time.

The second type of signal is the standard Telesonar signaling scheme which is known as MFSK. Although the details of the modulation are not pertinent to the navigation aid discussion, for completeness this is described by Figure 2. Here, we generate 32 tones for each baud period. The structure supports signaling from 140 bps to 2400 bps. Most users find that 600 bps to 800 bps suffices for most environments.

For the navigation-related signaling, such as a range request, we always use the 140 bps rate with an 8-byte packet.

There are auxiliary waveforms associated with the MFSK signal which are separate from the modulated portion. In particular, the modulated portion is preceded by several tones and a hyperbolic chirp. The latter is fundamental to three aspects of our combined communications and navigation schemes:

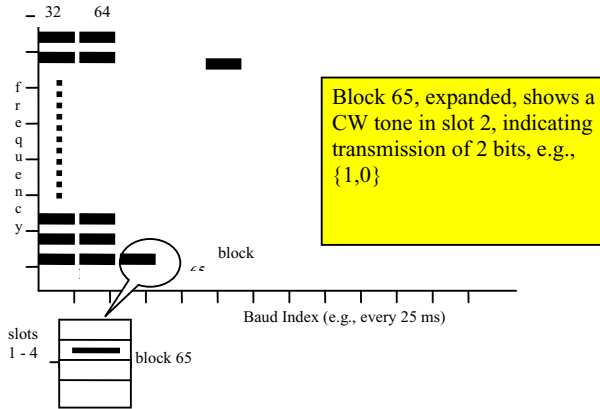


Fig. 2. Example of M=4 MFSK scheme transmitting two symbols with each tone

- 1 Temporal and spectral synchronization and range rate alignment.
 - a. Replica correlation-based processing, with additional processing described best in US Patent #7,218,574 “High Range Rate Signaling.”
- 2 Range measurement between two modems.
 - a. Range accuracy fundamentally limited by the inverse of the chirp bandwidth, which typically is 5120 Hz, or 0.2 ms in time.
 - b. Accuracy also depends on precisely known “turn-around time” within the electronics. This typically is known to within 0.05 ms error.
- 3 Bearing measurement of an arriving modem signal.
 - a. This is more fully described in section 3, following.

For completeness, the Telesonar modem also provides several varieties of phase shift keyed (PSK) signaling, with data rates between approximately 2500 bps to 10 kbps. Although all modems can transmit such waveforms, the receive algorithms (typically of the decision feedback (DFE) variety) are only available in a deckbox or buoy configuration.

3 Navigation Aids

Four different modem-based navigation aids are discussed in this section. The first provides a portable tracking range for verifying the internal navigation performance

of underwater vehicles. The second provides a translation of conventional satellite-based GPS to the underwater environment. The third provides a means for a platform to query a remote device to obtain position, and the fourth combines elements of the third to enable both group awareness (autonomy) and precision tracking of remote modems.

3.1 Portable Undersea Tracking System (PUTS)

The portable tracking range, under development for NUWC Keyport¹ since 2006, employs modems to provide real-time position information to submarines without the need for inter-node cabling, external processing or support systems that are required by existing ranges. This system, portrayed in Figure 3 is comprised of standard SM 75 units². For a submarine to determine its position, it transmits a “range” request with a conventional MFSK signal identifying up to 6 remotes in the message. The remotes respond with one of six FH signals available, depending upon the order in which the remotes were addressed. All 6 responses are processed simultaneously on the submarine to obtain ranges to each remote. Since the processor on the submarine is programmed with the geo-position of all remotes, it can then compute its position. This system includes a new transducer design and modem concept that utilizes just 2 wires between modem electronics and the transducer in place of the previous 8 wires. This, combined with a new deck-box containing a modem and other electronics, forms the core components of the submarine-based portion.

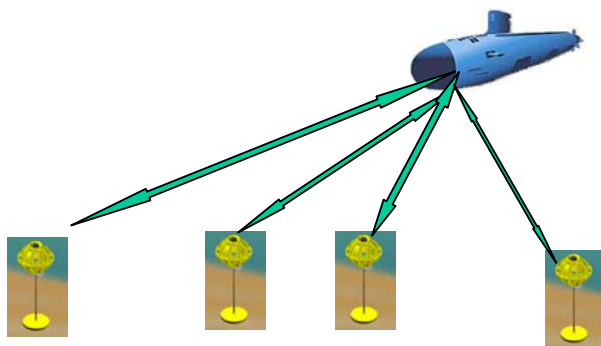


Fig. 3. Portable tracking range concept

A major consideration for PUTS success is the implementation of Benthos patented technology for accommodating high range rate (relative speed) encounters. This technology was developed with internal Teledyne funds, and has since become standard in all Telesonar and Seaweb modems.

¹ PUTS, SBIR Phase 3 contract N00253-06-R-0004, TPOC Mr. Doug Ray, NAVSEA Division Keyport, an OSD program.

² Smart Modem model 75.

3.2 Directional Acoustic Transponder (DAT) and Smart Marker

Although separate programs, the DAT and SM recently have been demonstrated together, so we discuss them together here. The Smart Marker (SM)³ project started in 2002 and developed a customized modem providing low-power extended operations for marking underwater objects. This is a “next-generation” marker that, in contrast to traditional analog responders, allows individually addressable units (in the same broad frequency band) using digital IDs for identification of individual units within a field, and the broadband signaling provides greater ranges and immunity to noise. Low-power and extended operations are enabled by reducing the modem’s power output and by the incorporation of advanced sleep modes.

The DAT is designed to be a single point replacement for a multi-node long baseline (LBL) navigation system. It operates in either of two ways. In the first, it queries a remote modem, or, in the present case a Smart Marker, returns a conventional modem ranging response. The DAT includes three (or more) small hydrophones used in a (modified) USBL method to estimate the arrival angle of the response. The two-way travel time is used to estimate the range. In the second method, a remote modem queries the DAT, which immediately estimates the bearing and returns that to the originating modem. Range is obtained from the two-way travel time. For the demonstration, the first method was used.

Figure 4 shows a solid edge drawing of the “wet end” of a DAT. The various components are indicated. Figure 5 shows a photograph of a Smart Marker. The total

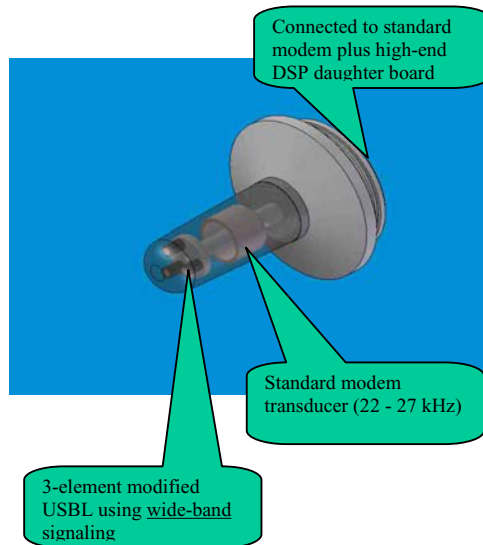


Fig. 4. DAT wet end, a portion of a system designed to provide communications, range, and bearing to and from a remote modem or Smart Marker

³ ONR SBIR topic N02-207 “Smart Marker”, phase II contract N00014-04-C-0111, Program Manager Dr. Thomas Swean (ONR), TPOC Dr. Brian Bourgeois (NRL).

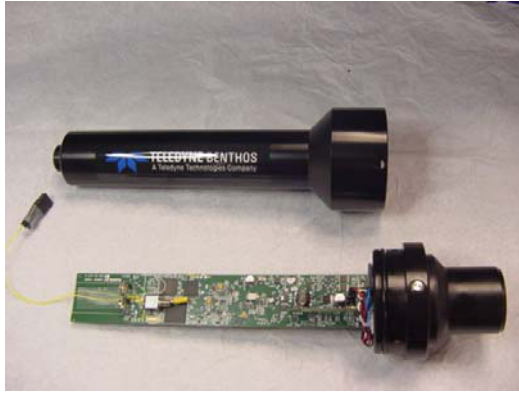


Fig. 5. Smart Marker, essentially a reduced size, lower power modem used as an object marker in underwater environments

length of the latter is approximately 30 cm. Both of these devices are designed to operate in the 22 – 27 kHz band, although lower frequencies are readily available as well.

A combined exercise was conducted with the DAT and the Smart Marker seaward of the surf zone in water between 3 and 8 meter depth. The DAT was placed on an underwater robotic crawler as shown in Figure 6. The Smart Marker was positioned on a 1 meter high tripod further out to sea. The crawler, towing a surface float and radio link and carrying a video camera, was driven through the surf. The DAT on the crawler was commanded to query the Smart Marker. Range and bearing were obtained. The crawler moved approximately 50% of the indicated range, along the direction indicated, then the DAT was queried again. This was repeated until the crawler moved DIRECTLY to the Smart Marker. The first acquisition occurred at 100 m range. As shown in this figure, the Smart Marker had toppled over and was partially buried in the sand. We note that an earlier exercise, which consisted of communicating with the Smart Marker from a nearby pier (shown in the figure), achieved perfect links at 328 m, at all of the available data rates, up to and including 2400 bps (true information rate). We thus assume that the crawler-based DAT would have found the marker from a considerably greater range had it not fallen over. We wish to emphasize that the crawler was commanded to follow precisely the DAT-indicated bearings. No “fudge factors” whatsoever were employed.

We note that the with the DAT carried on a cooperating fleet of underwater vehicles or divers, all participants obtain bearing to any other participant with each transmission, and any can query another for both range and bearing. This support UUV autonomy with both communications and location, and not only provides a group of divers with the same information, but as well provides the dive master with a real-time overview of the dive team’s locations and activities.

equipped with a GPS receiver (to obtain position, time, and 1 PPS signals), and an acoustic modem. At a specified instant (say, every 30 seconds), all of the modems simultaneously transmit their own positions using a Frequency hopping (multi-access) waveform. A passing vehicle with a modem on board, and without benefit of a synchronized clock, can extract each of the signals from the presence of the others and, knowing its own depth, can estimate its geo-position.

In this demonstration, we placed the three buoys in a northern portion of St. Andrews Bay and used a boat to carry an over-the-side modem as a surrogate UUV. The boat was kept at minimum forward speed, and conducted the exercise shown in part in Figure 7. Because the boat-based modem was equipped with its own GPS, we were able to develop a reasonable version of “ground truth,” as indicated by the red line. The blue line shows the estimate the UUV would make, given the same received geo-positions.

We note that our version of “truth” does not account for the error in buoy positions (derived from ordinary satellite GPS) nor for the towed modem, which was at least 4 meters (horizontal) and 3 meters (vertical) removed from the boat-based GPS receiver.

4 Summary

We have described several practical navigation aids, each based upon our core acoustic communications technology. Each has been demonstrated to be an effective, high performance alternative to existing conventional technology. The PUTS system, while still under development, has been repeatedly tested and shown to perform as designed – position accuracy is very good, and large scale deployments have been funded. The DAT, when carried on a UUV, is simple and easy to use. In this version it merely requires calibration to point to the nose of the vehicle. In the alternative version, it is placed on the sea floor as an addressable beacon, and calibration is provided simply by informing it acoustically of the direction of true North. At the frequencies used (22 – 27 kHz), it is small and unobtrusive, although we can provide a system at any frequency below this. The performance of the DAT is fundamentally limited by the physical size of the small hydrophones. At the current frequency they are rather large with respect to the carrier frequency wavelength. This development is continuing through new US Navy programs.

The Smart Marker performed flawlessly, both as a marker and as a modem. We have exciting opportunities to convert this marker into a new generation of “Compact Modem” for tagging and diver communications purposes, both of which are now under development.

The UW/GPS system performed very well. This is shown to be a reliable, easily-deployed, and unobtrusive system (the UUV only carries a modem). The buoys performed perfectly. As they have, in the past, carried RF modems as well, they are very suitable as gateway buoys for protected waters.

State-of-the-Art in MAC Protocols for Underwater Acoustics Sensor Networks*

Hung T. Nguyen, Soo-Young Shin, and Soo-Hyun Park**

Graduate School of BIT, Kookmin Univ.
bluekite315@yahoo.com, {sy-shin, shpark21}@kookmin.ac.kr

Abstract. Many potential applications such as ocean sampling network, environment monitoring, undersea exploration, disaster prevention, assisted navigation, and mine reconnaissance can be provided by deploying the Underwater Acoustic Sensor Networks. Because of the peculiarities of acoustic communication in underwater, the MAC protocol which play a role of managing and controlling the channels, must overcome the required of energy consumption, propagation delay and time synchronize as well as other factors. In this paper, we summarize and classify some current proposed MAC protocols as well as make a comparison table in order to bring out the current development of a very interesting research area. Beside, we briefly introduce our suggestion of MAC mechanisms for Underwater Acoustic Sensor Networks (UWASNs) named Gain-time and Guard-time TDMA mechanism and UWA-NAV mechanism.

Keywords: Underwater Acoustic Sensor Networks, Multiple Access Control, Medium Access Control, Schedule-based protocol, Contention-based protocol.

1 Introduction

The development of science and technology makes human's desire to conquer the ocean to be more reality by deploying the UWASNs. There many potential applications can be provided throught the networks such as ocean sampling network, environment monitoring, undersea exploration, disaster prevention, assisted navigation, and mine reconnaissance [1]. But the peculiarities of the physicals phenomena in ocean cause some challenges for the scientist when designing the UWASNs like, bandwidth limited, signal attenuation by multipath and fading effects, propagation delay, high bit error rates and temporary loss of connectivity, battery power limited, and underwater sensor failure [2]. These points require suitable architecture for underwater sensor network compare to terrestrial sensor network, especially in MAC protocol.

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the 2007 ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

** Corresponding Author.

MAC layer has the objectives of managing and controlling communication channels, which are shared by many nodes to avoid collisions and maintain reliable transmission condition. In terrestrial on air network, 40% of network utilization depends on MAC layer. But in UWASNs, MAC layer has more important affection on the network utilization. Because of the harsh environment in underwater, MAC protocol for UWASNs must overcome the required of energy consumption, propagation delay and time synchronize as well as other factors. Recently, many new scheduling and synchronization methods have been proposed to solve these problems.

In this paper we summarize the current proposed MAC protocols for UWASNs. The multiple access control including Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA) and the medium access control including ALOHA, Carrier Sense Multiple Access (CSMA), Multiple Access with Collision Avoidance (MACA), and Floor Acquisition Multiple Access (FAMA), which use in terrestrial sensor network, have been modified in order to adapt with the differences of acoustic transmission in underwater environment. Some typicality of current MAC protocols will be classified and introduced here. We hope that it will be a good reference for who have interesting in wireless sensor network, particularly in UWASNs.

This paper is organized as follows: Section 2 discusses about the multiple access control MAC protocols. Section 3 describes the medium access control MAC protocols. A comparison table in Section 4 will provide a summery in current development of MAC layer for UWASNs. Our proposed MAC mechanism for underwater acoustic sensor networks is presented in section 5. We give our conclusion in Section 6.

2 Multiple Access Controls

We make a distinction between multiple access controls schemes such as FDMA, TDMA, and CDMA, can be associated with the physical layer (PHY) and multiple access protocols, situated at the medium access control (MAC) above the PHY [3].

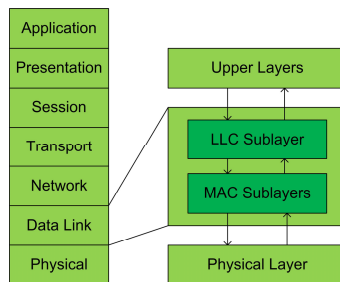


Fig. 1. Open systems interconnection reference model and data link layer architecture

In OSI layers shows in figure 1, the combination of multiple access controls schemes and medium access controls makes the MAC sub-layer. Roughly speaking, the scheme provide the capability of dividing the total resources available to a base station into individual portions, which can be assigned to different users, and the protocols govern access to the resource portions, e.g. provide access arbitration.

2.1 FDMA

In FDMA the system signaling are divided along the communication frequency into non-overlapping channels, and each user is assigned a different frequency channel. The channels often have guard bands between them to compensate for imperfect filters, adjacent channel interference, and spectral spreading due to Doppler. If the channels are sufficiently narrowband then even if the total system bandwidth is large, the individual channels will not experience frequency-selective fading [4].

The severe fading present in underwater acoustic channels creates a difficult environment for FDMA-based systems. And it is an inefficient protocol for the underwater environment because the limited bandwidth which was verified in the Seaweb project 1998 and 1999 [5]. For these reasons, FDMA is not suitable for UWASNs.

2.2 TDMA

TDMA is digital transmission technology that divides the communication frequency into time slots and then allocates unique time slots to each user. Users take turn transmitting and receiving in a round-robin fashion. It is worth noting, however, that only one user is actually using the channel at any given time for the duration of a time slot [6]. TDMA also has the advantage that it is simple to assign multiple channels to a single user by simply assigning him multiple time slots.

TDMA has good energy efficiency, but requires strict time synchronization and is not flexible to changes in the number of nodes. Due to the characteristics of the underwater environment it is very challenging to realize a precise synchronization, with a common timing reference, which is required for a proper utilization of time slots in TDMA. Moreover, due to the high delay and delay variance of the UWA channel, TDMA efficiency is limited because of the high guard time required to implement it.

2.3 CDMA

In CDMA the information signals of different users are modulated by orthogonal or non-orthogonal spreading codes. The resulting spread signals simultaneously occupy the same time and bandwidth. The receiver uses the spreading code structure to separate out the different users. The most common form of CDMA is multiuser spread spectrum with either direct sequence (DS) or frequency hopping (FH) [4].

CDMA is the most promising physical layer and multiple access technique for UWASNs since when it is robust to frequency-selective fading, compensates for the

effect of multipath by exploiting Rake filters at the receiver, and allows receivers to distinguish among signals simultaneously transmitted by multiple devices [7].

In the differences projects related to underwater acoustic communication realized by GESMA and its main partners, Sercel Bres ad ENST Bretagne, CDMA technique is carried out in 2003 and 2004 to provide underwater acoustic network with the ability to exchange data in multiple access environment [8]. This technique is a good choice for those who want to realize underwater acoustic communication in a multi-user context or long range acoustic transmission. According to the deterioration of spreading codes orthogonality brought by multipath, a Rake receiver is also used and evaluated during these sea-trials.

3 Medium Access Controls

The main objective of most MAC layer protocols is to reduce energy waste caused by collisions, idle listening, overhearing and excessive overhead. These protocols can be categorized into two main groups: contention based and schedule based MAC protocols. Contention based MAC layer protocol avoids pre-allocation of resources to individual users. Instead, a single communication channel is shared by all users and allocated on-demand. Simultaneous attempts to access the communication medium, however, results in collision. The main objective of contention based MAC layer protocol is to minimize, rather than completely avoid, the occurrence of collisions. To reduce energy consumption, these protocols differ in the mechanism used to reduce likelihood of a collision while minimizing overhearing and control traffic overhead. Schedule based protocol are class of deterministic MAC layer protocol in which access to the channel is based on a schedule. Channel access is limited to one user at a time. This is achieved based on pre-allocation of resources in to individual users [6].

3.1 Contention-Based MAC Protocols

3.1.1 ALOHA Based Protocols

The original ALOHA protocol is based on random access of users to the medium and do not try to prevent packet collision. Whenever a user has information to send, it transmits it immediately. This naturally leads to a large number of collisions, and hence a number of data packets have to be retransmitted. Therefore, the effective throughput of the ALOHA channel is very low because the probability of packet collisions is high. The Slotted ALOHA scheme was developed to deal with the collision problem. In Slotted ALOHA, the time is divided into slots, and packet transmission is restricted to these time slots. Thus, the number of collisions is reduced significantly. The throughput with Slotted Aloha is double that with basic ALOHA.

The limitation of ALOHA protocol in underwater environment was analyzed in the papers [9] and [10]. In [9], the paper presents a study on ALOHA and Slotted

ALOHA protocols for UWASNs. The results show that long propagation delay of acoustic signals prohibits the coordinate among nodes so it does not yield any performance gain. Although, the nodes sent the messages in pre-defined time slot, there is no guarantee that they will arrive in time slots. The simple analysis and simulation results show that Slotted ALOHA exhibits the same utilization as non-Slotted ALOHA. More over, in [10], the paper identifies the challenges of modeling contention-based medium access control protocols and presents a model for analyzing ALOHA variants for a simple string topology as a first step toward analyzing the performance of contention-based proposals in multi-hop underwater acoustic sensor networks. The limitation factor in the performance of ALOHA variants is collisions. Avoiding collisions is the goal of refinements to this protocols class.

In order to deploy the ALOHA protocol for UWASNs, adaptive improvements will be added to the original ALOHA overcoming the technical issues of this protocol. In [11] study the performance of ALOHA-based protocols in underwater networks, and propose two enhanced schemes, namely, ALOHA with collision avoidance (ALOHA-CA), and ALOHA with avoidance notification (ALOHA-AN), which are capable of using the long propagation delays to their advantage. Between two protocols, ALOHA-CA is simpler and more scalable, as it only needs a small amount of memory, and does not rely on additional control messages. ALOHA-AN, on the other hand, requires the use of additional notification (NTF) packets, which serve as advance notification to neighboring nodes, so that they can avoid transmitting packets that could result in collisions. The ALOHA-AN needs to collect and store more information, therefore it requires more resources than ALOHA. Simulation results have shown that both schemes can boost the throughput by reducing the number of collisions, and, for the case of ALOHA-AN, also by reducing the number of unproductive transmissions.

3.1.2 CSMA Based Protocols

In CSMA protocol, only one user can transmit at a time, on a first come, first served bases. When a user has a data to transmit it first listens to the medium and senses for a carrier on the medium to determine whether other users are transmitting: the carrier-sense phase. If the medium is busy, the user has to wait until the medium is idle. If no other users transmit data, the user proceeds to transmit its data onto the medium. However, when the medium is busy the user waits for a random of time (back-off time) after a collision before sensing the channel again. If two or more users simultaneously try to transmit, a collision of frames occurs, and all data is corrupted. In this case, all corresponding users stop transmitting. Therefore, after a collision, all the users involved will start contention, each after a randomly chosen amount of time. After finishing the transmission of data, a user waits for an acknowledgement (ACK) from the destination user. If the ACK does not arrive, the user retransmits the data [6].

In [12] the use of acoustic communication in terrestrial wireless sensor networks had been explored as an alternative way of communication among the motes. A light-weight, configurable MAC layer which adopts the principle of CSMA was developed

in order to facilitate the use of acoustic layer communication. The implementation of Acoustic MAC layer have the capability of snooping on traffic over the acoustic signals feature with a tone detector, automatic ACK after a node receives a package feature. A set of interfaces that allow network services to dynamically configure the Acoustic MAC is also provided. This research have meaningful because it showed some issues of acoustic communication not only in terrestrial wireless sensor network including receiver sampling period, sounder delay and saturation in tone detector but also much more important in UWASNs.

In [13], the multiple-access with collision avoidance and acknowledgment (MACAW) channel access approach for the MAC layer was proposed. The MACAW protocol relies on the exchange of request-to-send (RTS) and clear-to-send (CTS) packets to contend and secure the channel before a data packet is sent followed by an ACK packet. In implementing in such a scheme in ad hoc UWASNs, there is a proposed modification for multiple RTS in contention of the channel.

In [14] the authors also utilize a MAC protocol based on MACA that uses RTS/CTS/DATA/ACK handshaking along with carrier sensing. The protocol similar to MACA and FAMA in multiple communication channels in an Autonomous Underwater Vehicles (AUV) network. A variation of the MACA protocol called MACA-MCP since it utilizes Multiple Channels and Positioning information has been developed with performance enhancements through packet trains and position information exchange. This achieves a self-organizing clustered network behavior that lead to good efficiency and data rates per node in the underwater AUV.

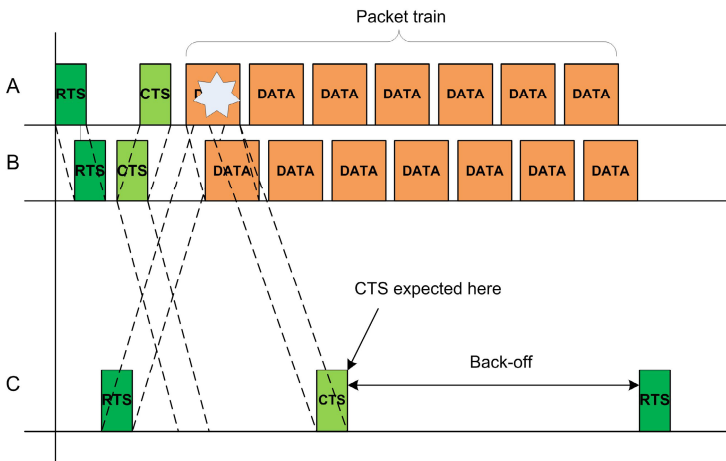


Fig. 2. MACA with DATA packet train improvement

The classical hidden node collision problem of MACA in Figure 2 can be solved by using packet train. The packet train in this case is a single large DATA packet. In such an RTS collision the entire DATA packet is lost and for re-transmission, the complete RTS/CTS/DATA/ACK exchange has to be repeated needlessly wasting

bandwidth. However, when packet trains are used, the RTS collisions only affect some of the packets in the train and the ACK will indicate this. By using fairly large number of packets in the train, efficiency can greatly be improved.

In [15], the paper proposed a MAC protocol suitable for an underwater acoustic network based on a channel access discipline called FAMA which combines both carrier sensing (CS) and dialogue between the source and receiver prior to data transmission. The new protocol uses time slotting and is thus called Slotted FAMA. Each packet (RTS, CTS, DATA or ACK) has to be transmitted at the beginning of one slot. The slot length has to be determined in a manner that ensures absence of data packet collisions. An ARQ protocol has also been included by sending ACK or NACK (Negative-acknowledgment) packets to acknowledge the data reception. Time slotting eliminates the need for excessively long control packets, thus providing savings in energy. Simulation results of this protocols show that for a given network topology, the transmission range can be chosen so as to maximize the network performance in terms of throughput and delay.

3.2 Schedule-Based MAC Protocols

In [16], the paper describes a new protocol for a network of acoustically-linked sub-sea sensors under the Acoustic Communication Network for the Monitoring of the Underwater Environment in Coastal Areas (ACME) project. The main aim of the project was to investigate the development of a system capable of operating in a harsh communication environment such as an estuary. ACME network protocol, ACMENet, is a master-slave protocol intended for small to medium sized UWASNs with arbitrary topologies. And MAC in ACMENet is based on scheduled transmission schedules that are designed such that data packets from slave nodes arrive at the master node consecutively, without collisions. CDMA scheme is used as an asynchronous multi-user transmission scheme where the nodes may be scheduled so that groups of synchronized data packet are received simultaneously. Each packet in the group will use a different orthogonal channel described by the multi-user scheme. Further, the transmission schedules are piggy-backed by special instructions to control the transmission power levels and modulation rates at slave nodes. Once all data packet have been received, the master node will then cause the sequence to be repeated by broadcasting other transmit instruction to the remote sensor nodes.

In [7] UW-MAC, a distributed MAC protocol for underwater acoustic sensor networks, was proposed. It is a transmitter-based CDMA scheme that incorporates a closed-loop distributed algorithm to set the optimal transmit power and code length. It is proven that UW-MAC manages to simultaneously achieve high network throughput, limited channel access delay, and low energy consumption in deep water communications, which are not severely affected by multipath. In shallow water communications, which are heavily affected by multipath, UW-MAC dynamically finds the optimal trade-off among these objectives.

In [17], the paper focus on design an energy-efficient MAC protocol for short range, acoustic sensor networks called "Tone Lohi". Lohi provides an energy conserving, throughput efficient, fair, and stable medium access for acoustic

networks. The energy is conserved in two ways: first, using data reservations to ensure no data packets collide. Second, employing wake-up tone hardware that resolves reservation contention with extremely low energy cost. Three flavors of T-Lohi representing different design choices also propose. By simulation, the results show that ST-Lohi (Synchronized T-lohi) is the most energy efficient protocol, within 3% of optimal energy. aUT-Lohi (Aggressive Unsynchronized T-Lohi) achieves the highest throughput (~50% channel utilization). cUT-Lohi (Conservative Unsynchronized T-Lohi) provides the most robust packet delivery with almost no packet loss. All three flavors exhibit efficient channel utilization, stable throughput, and excellent energy efficiency.

In [18], a distributed, scalable, energy-efficient MAC protocol that works despite long, unknown propagation delays of the underwater acoustic medium. This protocol can be used for delay-tolerant applications such as underwater ecological sensor networks between energy-limited nodes. The protocol differs significantly from ALOHA, MACA, and MACAW protocols in that energy is the main performance metric in the case rather than bandwidth utilization.

The proposed scheme was shown that provides at least 95% energy-efficiency in the MAC layer, when the number of 1-hop neighbors is about 6. For application, this MAC protocol will be combined with topology control for the operation of energy-limited sensor nodes in UWASNs.

3.3 Hybrid Protocols

In [19], the paper presents a multiple access scheme based on clustering which provides efficiency scalability by spatial reuse of channel resources. The network is partitioned into clusters, and transmissions in each cluster are scheduled following a TDMA algorithm. CDMA is used to enable spatial reuse of slots throughout the network. Network scalability is attained by reusing CDMA codes in distant clusters. Connectivity between nodes in different clusters is achieved using receivers that are capable of simultaneous detection at multiple spreading codes. The effect of CDMA processing gain on the network performance was quantified through the node connectivity/delay trade-off.

4 Comparison

In this section, we compare the protocols which describe in the early part. UW-MAC CDMA is the protocol that leverages CDMA properties to achieve multiple access in the bandwidth-limited underwater channel. Slotted FAMA with handshaking mechanism may lead to low system throughput and sensing an idle channel while in a transmission duration may cause packet collisions. MAC protocol in [18] has energy-efficient operation, but lacks effective mechanism for contention and is only suited for applications that have extremely low traffic rates.

Through following comparison table, we bring out a clear picture of the technique solutions using in these protocols in order to satisfy the requirement of collision avoidance, energy consumption and throughput that are very important measurements for the efficiency of a UWASNs.

Table 1. UWASNs MAC protocols’ specifics comparison

| Classification | Protocols | Network topology | Collision Avoidance | Energy consumption | Throughput |
|---------------------------|---|---|---|---|--|
| Contention based protocol | [11] ALOHA-CA with header segment and data segment, ALOHA-AN with advance notification packet | <ul style="list-style-type: none"> • Distributed topology | <ul style="list-style-type: none"> • Providing the local database table. | Saving by: <ul style="list-style-type: none"> • Not transmit packets may cause collision | Boost by reduce: <ul style="list-style-type: none"> • Collision • Number of unproductive transmissions |
| | [14] MACA with RTS / CTS/ DATA / ACK with carrier sensing | <ul style="list-style-type: none"> • Small AUV network | <ul style="list-style-type: none"> • Using short RTS and CTS • Better tuning of back-off timers | <ul style="list-style-type: none"> • Achieve efficiency | Increase data rate due to: <ul style="list-style-type: none"> • Dividing the traffic across the multiple channels • Optimizing packet train size |
| | [15] Slotted FAMA with carrier sensing (CS) and a nodes’ dialogue | <ul style="list-style-type: none"> • Mobil ad hoc underwater network | <ul style="list-style-type: none"> • RTS or CTS within transmission range over one slot | Saving energy due to: <ul style="list-style-type: none"> • Eliminating long excessive control packets • Idle state of terminals in time slots | <ul style="list-style-type: none"> • Achieved maximum around 2 km distance |
| Schedule based protocol | [7] UW-MAC CDMA using closed-loop distributed algorithm | <ul style="list-style-type: none"> • Two-dimensional deep water • Three-dimensional shallow water | <ul style="list-style-type: none"> • Small EH randomly accessing the channel | Optimal transmit power by: <ul style="list-style-type: none"> • Have a low number of packet retransmissions | High network throughput due to: <ul style="list-style-type: none"> • High channel reuse |
| | [17] Tone Lohi with reservation tone and wake-up tone | <ul style="list-style-type: none"> • Differences underwater sensor network architecture scenarios | <ul style="list-style-type: none"> • Reservation | Reduce the energy by: <ul style="list-style-type: none"> • Using wake-up tone detection | <ul style="list-style-type: none"> • Efficient at low load • Stable at high load |
| | [18] Distributed, scalable, energy-efficient MAC protocol | <ul style="list-style-type: none"> • Dense network of hundreds of sensors | <ul style="list-style-type: none"> • SYNC packet • Guard time duration. | Saving nodes energy due to: <ul style="list-style-type: none"> • Sleep mode • Low duty cycles | Have low throughput by: <ul style="list-style-type: none"> • Spending time to wake up sleep nodes |

5 Suggestion Mechanism of the UWASNs MAC

5.1 GT^2 TDMA MAC

Common problem of underwater environment is a propagation delay regardless of what kinds of MAC are used. That is, the problem of propagation delay is not related to communication protocols. Generally, a Guard-time has been applied based on the maximum propagation delay of the network. However, our Gain-time and Guard-time (GT^2) TDMA MAC scheduling proposed technique can be applicable to clustered networks. The proposed method is to increase the network efficiency by determining the moment of data Gain-time and Guard-time in to consideration [23].

5.2 UWA-NAV: Energy Efficient Error Control Scheme for Underwater Acoustic Sensor Network

Since there are various disturbing factors such as long propagation delay and high error rate in UW-ASN, an error control mechanism is required to improve the system performance efficiently. The carrier sensing technique, which detects whether the public media access is already occupied or not and evade the collision, is used as an error control mechanism. A method of monitoring the energy level of wireless frequency in physical layers and a method of setting-up NAV (Network Allocation Vector) using the frame transmission period were modified and re-defined for underwater environment. Through these works, a more efficient UWA-NAV technique was able to be proposed and the performance of the proposed technique was evaluated and compared with the case without UWA-NAV [24].

6 Conclusion

This paper reviews the current development of MAC protocols for Underwater Acoustic Sensor Networks. These protocols were introduced and classified by legacy MAC scheme likes contention-based protocols and schedule-based protocols. A table also was added in order to bring a comparison between specifics of the represent UWASNs MAC. We also implement our proposed GT^2 TDMA and UWA-NAV MAC mechanisms.

Our researches are still going on the Underwater Acoustic Sensor Networks project 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). Our future work including simulation our proposed MAC mechanisms (GT^2 and UWA-NAV), experiment in the filed test in the sea with fully implementation by using MSP430 microcontroller, acoustic modem as well as others hardware and software. We also will execute the comparison between simulation and experiment in order to take the implementation for our mechanisms.

References

- [1] Akyildiz, I.F., Pompili, D., Melodia, T.: Underwater acoustic sensor networks: research challenges, *Ad Hoc Networks*, vol. 3(3), pp. 257–279. Elsevier, Amsterdam (2005)
- [2] Akyildiz, I.F., Pompili, D.: State-of-the-art in protocol research for underwater acoustic sensor networks. In: *WUWNet 2006. Proceedings of the 1st ACM international workshop on Underwater networks* (2006)
- [3] Brand, A., Aghvami, H.: *Multiple Access Protocols for Mobile Communications: GPRS, UMTS and Beyond*. Wiley Publication (2002)
- [4] Wu, S.L., Tseng, Y.C.: *Wireless Ad Hoc Networking: Personal-Area, Local-Area, and the Sensory-Area Networks*, 1st edn. Auerbach Publications (March 2007)
- [5] Rice, J., et al.: Evolution of Seaweb Underwater Acoustic Networking. In: *Oceans Conf.*, Providence, RI, pp. 2007–2017 (2000)
- [6] Sohraby, K., Minoli, D., Znati, T.: *Wireless Sensor networks: Technology, Protocols, and Applications*. Wiley Publication, Chichester (2007)
- [7] Pompili, D., Melodia, T., Akyildiz, I.F.: A Distributed CDMA Medium Access Control for Underwater Acoustic Sensor Networks. In: *Proc. of Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, Corfu, Greece (2007)
- [8] Lapierre, G., Beuzelin, N., Labat, J., Trubuil, J., Goalic, A., Saoudi, S., Ayela, G., Coince, P., Coatelan, S.: 1995-2005: Ten years of active research on underwater acoustic communications in Brest. In: *Oceans 2005 - Europe*, vol. 1, pp. 425–430 (June 20-23, 2005)
- [9] Vieira, L.F.M., Kong, J., Lee, U., Gerla, M.: Analysis of ALOHA protocols for underwater acoustic sensor networks. In: *WUWNet. The First ACM International Workshop on UnderWater Networks* (2006)
- [10] Gibson, J.H., Xie, G.G., Xiao, Y., Chen, H.: Analyzing the Performance of Multi-hop Underwater Acoustic Sensor Networks. In: *Proc. MTS/IEEE Oceans 2007 Conference*, Scotland (June 2007)
- [11] Chirdchoo, N., Soh, W.S., Chua, K.C.: ALOHA-based MAC Protocols with Collision Avoidance for Underwater Acoustic Networks. In: *INFOCOM 2007, 26th IEEE International Conference on Computer Communications*, IEEE, Los Alamitos (2007)
- [12] Zhang, J., Huang, Z., Liu, X.: Acoustic Communication in Wireless Sensor Networks. Department of Computer Science University of Virginia, CS651, *Wireless Sensor Networks (TA Course)* (December 2005)
- [13] Foo, K.Y., Atkins, P.R., Collins, T., Morley, C., Davies, J.: A routing and Channel-Access Approach for an Ad Hoc Underwater Acoustic Network. In: *OCEANS 2004. MTS/IEEE TECHNO-OCEAN 2004*, vol. 2, pp. 789–795 (November 9-12, 2004)
- [14] Shahabudeen, S., Chitre, M., Motahi, M.: A multi-channel MAC protocol for AUV networks. In: *Oceans 2007*, Aberdeen (June 2007)
- [15] Molins, M., Stojanovic, M.: Slotted FAMA: a MAC Protocol for Underwater Acoustic Networks. In: *OCEANS. Proc. of MTS/IEEE Conference and Exhibition for Ocean Engineering, Science and Technology*, Boston, MA (September 2006)
- [16] Adams, A.E., Acar, G.: An Acoustic Network Protocol for Sub-Sea Sensor Systems. In: *IEEE Oceans 2005 Europe Conference*, Brest (2005)
- [17] Syed, A.A., Ye, W., Heidemann, J.: T-Lohi: A New Class of MAC Protocols for Underwater Acoustic Sensor Networks, in *Technical Report ISI-TR-638*, USC/Information Sciences Institute (April 2007)

- [18] Rodoplu, V., Park, M.K.: An Energy-Efficient MAC Protocol for Underwater Wireless Acoustic Networks. In: OCEANS. Proc. Of MTS/IEEE Conference and Exhibition for Ocean Engineering, Science and Technology (September 2005)
- [19] Salva-Garau, F., Stojanovic, M.: Multi-cluster Protocol for Ad Hoc Mobile Underwater Acoustic Networks. In: Proc. of MTS/IEEE OCEANS, San Francisco, CA (September 2003)
- [20] Sozer, E., Stojanovic, M., Proakis, J.: Underwater Acoustic Networks. *IEEE Journal of Oceanic Engineering* 25(1), 72–83 (2000)
- [21] Heidemann, J., Ye, W., Wills, J., Syed, A., Li, Y.: Research challenges and applications for underwater sensor networking. In: WCNC 2006. Wireless Communications and Networking Conference, vol. 1, pp. 228–235. IEEE, Los Alamitos (2006)
- [22] Partan, J., Kurose, J., Levine, B.N.: A survey of practical issues in underwater networks. In: WUWNet 2006. Proceedings of the 1st ACM international workshop on Underwater networks, pp. 17–24. ACM Press, New York (2006)
- [23] Shin, S.Y., Park, S.H.: GT2: Reduced Wastes time Mechanism for Underwater Acoustic Sensor Network. In: Denko, M., et al. (eds.) EUC Workshops 2007. LNCS, vol. 4809, Springer, Heidelberg (2007)
- [24] Shin, S.Y., Park, S.H.: UWA-NAV: Energy Efficient Error Control scheme for Underwater Acoustic Sensor Network. In: Denko, M., et al. (eds.) EUC Workshops 2007. LNCS, vol. 4809, Springer, Heidelberg (2007)

An Ultrasonic Sensor Based Low-Power Acoustic Modem for Underwater Communication in Underwater Wireless Sensor Networks

Heungwoo Nam and Sunshin An

Computer Network Lab., Dept. of Electronics Engineering, Korea University
1, 5-Ga, Anam-dong, Sungbuk-gu, Seoul, Korea, Post Code: 136-701
{hwnam, sunshin}@dsys.korea.ac.kr

Abstract. Applications of underwater sensor networks involve environmental monitoring, disaster prevention, and resource detection. As the importance of these applications has recently grown, underwater sensor networks made up of sensor nodes have to be further investigated. However, little research has been performed to develop an underwater sensor node with communication functionality. In an underwater environment, typical RF-based communication is not appropriate because of two facts. One fact is that radio waves require large antennae and high transmission power. The other fact is that the Berkeley Mica 2 Motes have been reported to have a transmission range of 120cm underwater. Consequently, we have concluded that underwater communication has to use an acoustic or ultrasonic wave rather than a radio wave. The objective of our work is to develop an acoustic modem for underwater communication, where we have to consider an energy-aware acoustic modem. This is because the battery can not easily be recharged underwater as well as in a terrestrial environment. As a consequence, an acoustic modem has to be designed with low-power. In this paper, we describe our implementation of an energy-aware acoustic modem and its performance in underwater experiments.¹

Keywords: Underwater communication, Acoustic modem.

1 Introduction

Recent advances in processors, memory, and radio technology have made smart, tiny, and cheap nodes possible. Wireless sensor networks composed of these nodes can be used in promising network architectures. These sensors also collect a number of useful information in an unattended manner. Applications of underwater sensor networks are composed of environmental monitoring, disaster prevention,

¹ This research was supported by the MIC (Ministry of Information and Communication), Korea, under the 2007 ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

and resource detection. As the importance of these applications has recently grown, underwater sensor networks made up of sensor nodes have to be further investigated. However, little research has been conducted in developing the underwater sensor node with communication functionality.

In an underwater environment, typical RF-based communication is not appropriate because of two facts. The first fact is that radio waves require large antennae and high transmission power. The other fact is that the Berkeley Mica 2 Motes, the most popular experimental platform, have been reported to have a transmission range of 120cm in underwater at 433MHz [1]. Consequently, we have concluded that underwater communication has to use an acoustic or ultrasonic wave rather than a radio wave.

The objective of our work is to develop an acoustic modem for underwater communication, where we have to consider an energy-aware acoustic modem. That is because the battery can not be recharged underwater as well as in a terrestrial environment. As a consequence, the acoustic modem has to be designed with low-power. In this study, we implemented the energy-aware acoustic modem.

The contributions of this paper are as follows. First, this work develops a low-power based acoustic modem. In particular, our modem operates with a 3.3V power supply. To that end, the lifetime of a sensor node was prolonged. Second, the modem for our study is a low-cost based acoustic modem with the capability for digital data communication. Because there is no existing modem with this capability based on low-cost, our modem is significant in this respect. Third, our work provides the basis for a ubiquitous device underwater as well as in a terrestrial environment. That is, the modem is smarter, smaller, and cheaper for underwater as well as terrestrial uses. As a result, this work's results are significant, including the result of having a technical method to perform real-time underwater monitoring effectively.

The remainder of this paper is organized as follows. Section 2 addresses related work on acoustic modems. In Section 3, we describe design principles and a hardware implementation of an acoustic modem. Section 4 describes underwater communication using software. The performance evaluation via underwater experiment is presented in Section 5. The comparisons and design challenges are provided in Section 6. In Section 7, we give some conclusions and future work.

2 Related Work

Acoustic communication plays an important role in underwater applications such as environmental monitoring, disaster prevention, and resource detection. Currently, underwater acoustic communication has received significant attention from many researchers. Previously, existing acoustic modems such as [2] [3] are commercial acoustic modems. However, they are usually bulky and expensive. They are not designed with low-power and they consume large amounts of

energy. From this fact, we concluded that long-lived sensor networks over battery-powered nodes could not be implemented. In our state-of-the-art design, we focus on a low-power and low-cost acoustic modem.

There are acoustic modems designed with low-power. The authors in [4] proposed CORAL. It uses special acoustic hardware which consists of piezo-transducers, a microcontroller-based architecture and interface circuitry. However, the difference between CORAL and our modem is the power supply. While the power supply of CORAL is 5V, the power supply of our modem is 3.3V. The authors in [5] proposed a Mica2 Sensor Board with an integrated Sounder and Microphone. In fact, their power supply in this system is similar to that in our modem. However, this system could not be used in underwater communication. The authors in [7] proposed a low-power acoustic modem. However, the power supply of this modem is 5V. Also, this modem does not perform underwater testing.

Different from the above, our modem uses ultrasonic sensors and its power supply is 3.3V. Also by taking the underwater test, it proves, itself, with underwater usage.

3 A Hardware Implementation of an Acoustic Modem

First, we now discuss the design principles of an acoustic modem. Our modem design includes several principles as follows. These principles are used to perform underwater communication effectively. i) Low-power based modem: Sensor networks composed of sensor nodes are based on a low-power design. Batteries can not be recharged underwater. Thus, to allow the long-lived operation of sensor nodes, we have to design a low-power modem. ii) Low-cost based modem: In our study, we found commercial acoustic modems usually bulky and expensive. We concluded that commercial acoustic modems did not allow for much wider deployment. Also, devices such as a submarine and an autonomous underwater vehicle (AUV) used acoustic communication, but were expensive. We, therefore, have to make a low-cost modem for wider dissemination. iii) Modem with the capability for digital data communication: Most underwater communications has been accomplished by sending only analog data such as voice. There is no underwater communication using a microcontroller which processes digital data. That is why many researchers investigate underwater communications sending digital data. Hence, by this fact, we have to develop an acoustic modem to communicate digital data by means of a microcontroller.

This work implements an underwater acoustic modem according to the above design principles. The microcontroller for the sensor node is an ATmega128L, which has an 8bit MCU, and operates from a 3.3 volt power supply. Hence, the power supply of our underwater modem is also 3.3 volt.

Fig. 1 shows a block diagram of an acoustic modem. Our acoustic modem is divided into two main parts: an ultrasonic transmitter and an ultrasonic receiver. These parts used ultrasonic sensors to generate or detect the ultrasonic wave. The ultrasonic sensors, which are waterproof, use a 40 kHz frequency both for

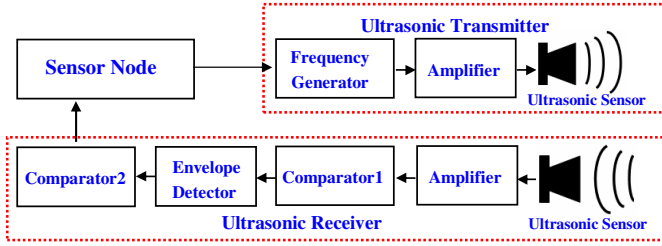


Fig. 1. A block diagram of an acoustic modem

the transmitter sensor and the receiver sensor. We, next, describe the details of this ultrasonic transmitter and receiver.

3.1 Ultrasonic Transmitter and Receiver

The ultrasonic transmitter consists of three components: a frequency generator, an amplifier, and an ultrasonic sensor. The frequency generator makes a 40 kHz frequency and uses an ASK modulation/demodulation method that combined an on-off voltage level with a carrier wave. Then, the modulated signals in the frequency generator are sent to the amplifier. The amplifier amplifies these input signals. The voltage level of the amplified signals is $-6V \sim +6V$. Finally, the ultrasonic sensor transmits these amplified signals.

The ultrasonic receiver is composed of five components: an ultrasonic sensor, an amplifier, an envelope detector, and two comparators. The ultrasonic sensor receives the transmitted signals and sends them to the amplifier. Because the received signals are a minute signal, to process them in the next step, they have to be amplified. So, the amplifier amplifies the received signals. Then, the comparator1 removes the noise from the amplified signals and sends the signals to the envelope detector. The envelope detector detects the original signals from the amplified signals. Finally, the comparator2 transforms these analog signals into digital signals and sends them to the sensor node. The sensor node uses software to regenerate the transmitted data.

4 Underwater Communication Software

4.1 Packet Format

We use a packet which is composed of two flags, a payload header and a payload. Here, two flags carry out the functionality of an acoustic physical layer header. A payload header performs the functionality of an acoustic MAC layer header. That is why we are able to make up the compact packet and carry out the test.

Fig. 2 shows our packet format. For more explanation, we describe all the elements of the packet.

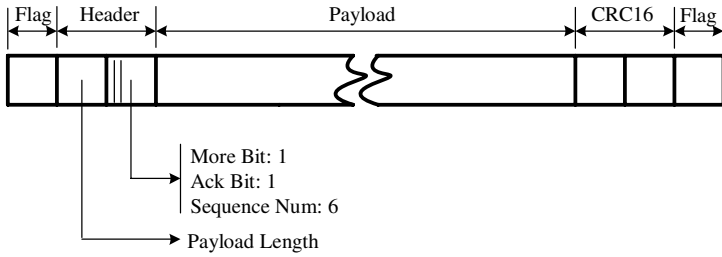


Fig. 2. The packet format

- **Flag:** The flag uses a bit sequence of 11011011. It is used to indicate the start and end of a packet. The length of the flag is 1 byte. The start bit of the flag is 1. This makes a sensor node know that a packet arrives. So, the sensor node generates an interrupt to perform a software sampling method which is provided in Subsection 4.4.
- **Payload length:** The payload length is the size of the payload. It has 1 byte.
- **More bit:** The more bit is used to recognize the end of the packet. Its length is 1 bit.
- **Ack bit:** The ack bit is used to distinguish between the data packet and the ack packet. The length of the ack bit is 1 bit.
- **Sequence number bit (SNB):** The sequence number bit shows the order of each packet. It has 6 bits.
- **CRC (Cyclic Redundancy Check):** The CRC is at end of the packet. In our implementation, we use CRC16, which has 2 bytes, to detect the transmitting errors. The value of CRC16 is extracted from CRC16-Table which is made up of 256 elements.

The length of the payload is not fixed. Its length is decided according to the kind of applications. This work uses a 20 bytes payload to carry out the underwater communication. In this experiment, we do not consider a number of MAC services. These MAC services will be left for future work.

4.2 The Transmitted Signals in the Ultrasonic Transmitter

The modulation method used in this work is an ASK. The ASK identifies whether the signal is sent or not, and generates the signal according to this fact. For example, when transmitting the bit '1', the frequency generator generates 40 kHz during t time. Otherwise, it does not generate the frequency during t time. That is, the frequency generator uses an on/off method according to the data from the MCU and transmits the data. For more explanation we provide Fig. 3. The amplifier uses the RS232 IC to amplify the signals which come from the frequency generator. Fig. 3 shows these amplified signals.

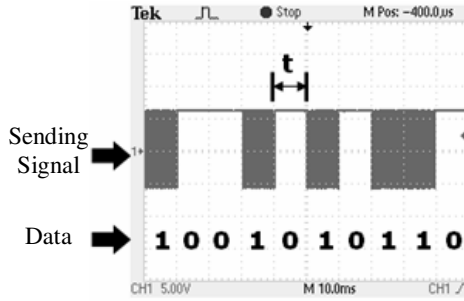


Fig. 3. The signals in the amplifier

Here, we define the sending period, t time (ms). This time is defined as the time interval of transmitting each bit. Thus the data rate is denoted in Formula (1):

$$DataRate = 1000/t \tag{1}$$

If the performance of the ultrasonic sensor is high, the data rate will be improved much more. This will be explained in Section 5.

4.3 The Received Signals in the Ultrasonic Receiver

The ultrasonic sensor receives the transmitted signals and sends them to the amplifier. Because the received signals are a minute signal, they have to be amplified. Fig. 4(a) shows the amplified signal in the amplifier. Then, the comparator1 removes the noise. The envelope detector detects the original signals from the amplified signals. Finally, the comparator2 transforms these analog signals into digital signals and sends them to the sensor node. The demodulated signal, later to be transmitted to the sensor node, in the comparator2 is shown

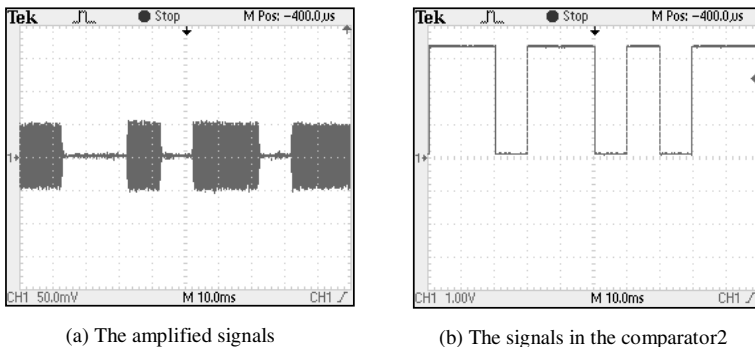


Fig. 4. The signals in the receiver part

in Fig. 4(b). These signals are entered into the comparator port in the sensor node. The sensor node uses software to retrieve the original data.

4.4 The Software Sampling Method

The signals, which are shown in Fig. 4(b), are entered into the comparator port in the sensor node. The comparator port uses a software sampling method to interpret these signals as the original signals. The software sampling method is as follows. The comparator port generates an interrupt at an interval of $t/2$ time from the high toggled signal to read the entered signal. Next, the port reads the entered signal at regular intervals of t time. For a more detailed explanation, we provide Fig. 5 which shows the software sampling method. Thus, if the value of the signal is greater than the value of the comparator, the comparator port represents the signal as 1. Otherwise, the port identifies it as 0.

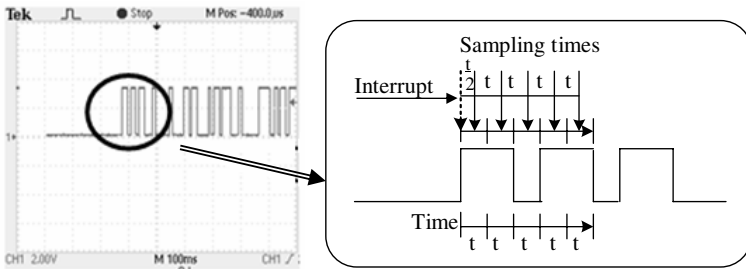


Fig. 5. The software sampling method

5 Performance Evaluation

5.1 Test Environment for Underwater Communication

We used an aquarium to perform underwater communication. Fig. 6 shows the test environment. Fig. 6(a) is a picture of the overall system. For more explanation, we illustrate with Fig. 6(b). Two notebooks were connected with two sensor nodes which were linked to the acoustic modems in the water. The sensor node used the ATmega128L MCU. In the near future, these sensor nodes will be put in the water. The notebook used the UART to communicate with the sensor node. The UI was a hyper-terminal. The underwater communication between the sensor nodes was performed by sending text.

The communication experiment was conducted with the following steps. First, in the transmitter part, we inputted the data to be transmitted in the notebook. Then, the sensor node sent the data to the acoustic modem. The acoustic modem transformed the data into an analog signal and transmitted it through the ultrasonic sensor. In another receiver part, the acoustic modem amplified the

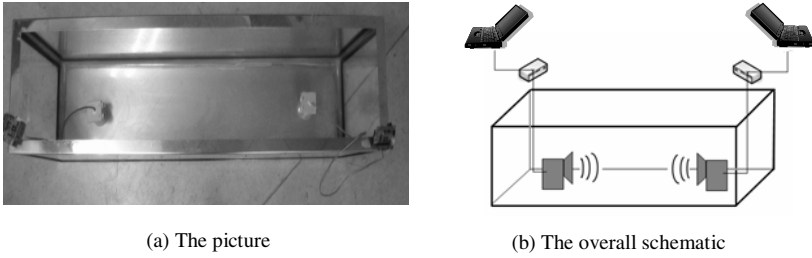


Fig. 6. The test environment

signals received by the ultrasonic sensor and transformed the amplified signals into digital signals. Then, the sensor node interpreted the digital signals and sent them to the notebook. Finally, we identified the transmitted data in the notebook.

5.2 The Sending Period and Communication Distance

Based on our test environment, we carried out the experiments by changing the sending periods. In our experiments, the length of the payload was set to 20 bytes. For each sending period, the transmitter sent 100 packets to the receiver. The receiver recorded the number of the packets received correctly to compute the packet delivery ratio.

Fig. 7 shows the different packet deliver ratios when the sending period changed. As shown in the figure, the packet delivery ratio increased as the sending period increased. For a 10ms sending period, we obtained a packet deliver

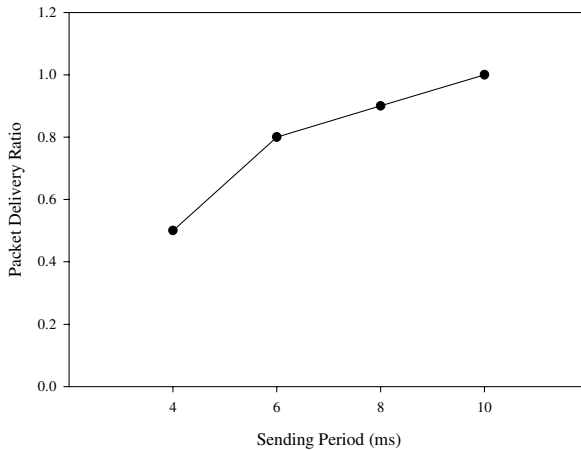


Fig. 7. Packet delivery ratio vs. the sending period

ratio 1. This means that the packet deliver error is not generated. So, we define the data rate of our modem as 100 bps. If the acoustic modem can be improved in the ultrasonic sensors, we can decrease the sending period to increase the data rate. This remains for future work.

We did not consider the communication distance. That was because we focused on whether our modem operated very well or not. Fortunately, the communication distance of our modem was $3m$. Therefore, finding the exact range of the acoustic modem would have required an enlarged test facility.

6 The Comparisons and Design Challenges

To evaluate the performance of our acoustic modem, we provide Table 1. Table 1 has the evaluations of and comparisons of the performance of the acoustic modems. Because these modems were very recently developed with low-power and low-cost, we compared them so that we could represent the superiority of our modem from the performance perspective.

The comparisons of the acoustic modems are as follows. First, the power supply of our modem was 3.3V, and all the others had a 5V power supply. Here, we did not know the power supply of the acoustic communication [5]. So, we inferred its power supply from the usage of the sounder and microphone as used in low-power acoustic modem [7]. In the energy consumption perspective, our modem was the best of all the others. Second, while our modem and the CORAL [4] were used in the underwater experiment, the Acoustic Communication [5] and the Low-Power Acoustic Modem [7] were not performed in the underwater test. Also, while the test of CORAL [4] put only sensors in the water, our test involved testing the acoustic modem and sensors in the water. From an objective point of view as to the number of devices in the water, our test was much more concerned with the underwater experiment. Third, while the data rate of our modem was 100bps, the data rate of the Acoustic Communication [5] was less than 10bps. By this fact, the data rate of our modem was ten times as fast as that of the Acoustic Communication [5]. We did not know the data rate of the CORAL [4] and the Low-Power Acoustic Modem [7]. From the viewpoint of the data rate, our modem had the best performance. Fourth, the frequencies of the CORAL [4], the Acoustic Communication [5], the Low-Power Acoustic Modem [7], and our modem were 1.7 kHz, 4.5 kHz, 18 kHz, and 40 kHz respectively. Finally, the transmitting/receiving devices of the CORAL [4], the Acoustic Communication [5], the Low-Power Acoustic Modem [7], and our modem were the piezo-transducers, the sounder and microphone, the projector/speaker and hydrophone/microphone, and the ultrasonic sensors respectively. So, only our modem used the ultrasonic sensors. As the above comparison indicated, we concluded that the functionality of our acoustic modem came significantly forward in the power supply, the underwater experiment, and the improved data rate aspects.

The design challenges to overcome for the underwater modem are as follows. i) The directional property: The directional property of the ultrasonic sensor is so

Table 1. A comparisons of the acoustic modems

| Acoustic Modem | Power Supply (Microcontroller) | Underwater Experiment | Data Rate (bps) | Freq- uency (kHz) | Transmitting /receiving Device |
|------------------------------|--------------------------------|--------------------------------|-----------------|-------------------|--|
| CORAL [4] | 5V (TI MSP430) | O (only sensors) | - | 1.7 | Piezo-transducers |
| Acoustic Communication [5] | 5V (MICA2 Mote) | X | <10 | 4.5 | Sounder, Microphone |
| Low-Power Acoustic Modem [7] | 5V (MICA2 Mote) | X | - | 18 | Projector/ Speaker, Hydrophone/ Microphone |
| Our acoustic Modem | 3.3V (ATmega128L) | O (acoustic modem and sensors) | 100 | 40 | Ultrasonic Sensors |

sensitive that if the direction is not matched, its transmitting error is increased. To that end, the pinpoint development of an ultrasonic sensor is needed. The underwater acoustic modem also has to process a minute signal. ii) The reflection and refraction: The reflection and refraction of a signal in underwater are very hard. That is why underwater communication is more difficult than terrestrial communication. The underwater acoustic modem has to remove the noise such as the reflection and refraction.

7 Conclusion and Future Work

Through related work, we knew the requirement that the underwater sensor networks must perform the acoustic communication. According to this requirement, this research with regard to an acoustic modem has significant meaning when performing acoustic communication. However, the hardware to support acoustic communication did not exist at all prior to our work.

This work developed an acoustic modem as hardware to perform acoustic communication. Thus, the advantages of our acoustic modem are as follows. First, our acoustic modem is a low- powered acoustic modem. In the energy consumption perspective, our modem was the best of all the others. Second, our modem is a low-cost based acoustic modem with the capability of digital data communication. Because there had been no prior existing modem with this

capability based on low-cost, our modem is significant in this regard. Through Table 1, we do know the fact that our modem come to the fore among the acoustic modems which have developed recently.

Some of the problems to be considered in our acoustic modem are: the directional property, the reflection, and the refraction. Our future work is the research to overcome these problems. Because the underwater applications have significant attraction of themselves, the acoustic modem with the functionality of the underwater communication will become much more significant. Therefore, it is our task to develop the acoustic modem to its fullest potential. In addition, this acoustic modem will become the basis for the underwater wireless sensor networks.

References

1. Akyildiz, I.F., Pompili, D., Melodia, T.: Underwater Acoustic Sensor Networks: Research Challenges. Elsevier's Journal of Ad Hoc Networks 3(3), 257–281 (2005)
2. Benthos, Inc., Fast And Reliable Access To Undersea Data, <http://www.benthos.com/pdf/Modems/ModemBrochure.pdf>
3. LinkQuest, Inc., Underwater Acoustic Modems, http://www.link-quest.com/html/uwm_hr.pdf
4. ya, Engel, J., Chen, J., Fan, Z., Liu, C.: CORAL: Miniature Acoustic Communication Subsystem Architecture for Underwater Wireless Sensor Networks. In: The 4th IEEE International Conference on Sensors (October 2005)
5. Zhang, J., Huang, Z., Liu, X.: Acoustic Communication in Wireless Sensor Networks. In: CS651, Wireless Sensor Networks, pp. 1–8 (December 2005)
6. Crossbow Technologies, Inc., <http://www.xbow.com/>
7. Wills, J., Ye, W., Heidemann, J.: Low-Power Acoustic Modem for Dense Underwater Sensor Networks. In: Proceedings of the First ACM International Workshop on Underwater Networks (WUWNet), pp. 79–85 (September 2006)

UWA-NAV – Energy Efficient Error Control Scheme for Underwater Acoustic Sensor Network*

Soo-Young Shin and Soo-Hyun Park**

Graduate School of BIT, Kookmin University
{sy-shin, shpark21}@kookmin.ac.kr

Abstract. Since there are various disturbing factors such as long propagation delay and high error rate in UW-ASN, an error control mechanism is required to improve the system performance efficiently. In this paper, the carrier sensing technique, which detects whether the public media access is already occupied or not and evade the collision, is used as an error control mechanism. A method of monitoring the energy level of wireless frequency in physical layers and a method of setting-up NAV (Network Allocation Vector) using the frame transmission period were modified and re-defined for underwater environment. Through these works, a more efficient UWA-NAV technique was able to be proposed and the performance of the proposed technique was evaluated and compared with the case without UWA-NAV.

Keywords: UW-ASN, NAV, Congestion Control, Error Control, Energy Aware.

1 Introduction

The connection technology of IEEE 802.11x has adopted CSMA/CA (Carrier Sensing Multiple Access / Collision Avoidance) technique. CSMA/CA uses carrier sensing technique for identifying whether the transmission media is used by other nodes or not. There are two methods of carrier sensing. One method is monitoring energy level of wireless frequency at physical layer. Another method specifies NAV (Network Allocation Vector) using frame transmission period virtually. It is called virtual carrier sensing. NAV means remaining time of current transmission session. Through NAV, it can be detected whether other nodes are transmitting or not. In other word, if NAV is set up then it means that the transmission route is occupied by some nodes[1][2].

The proposed concept of UWA-NAV in underwater sensor network is different from that of wireless communication. The proposed method occupies the transmission

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the 2007 ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

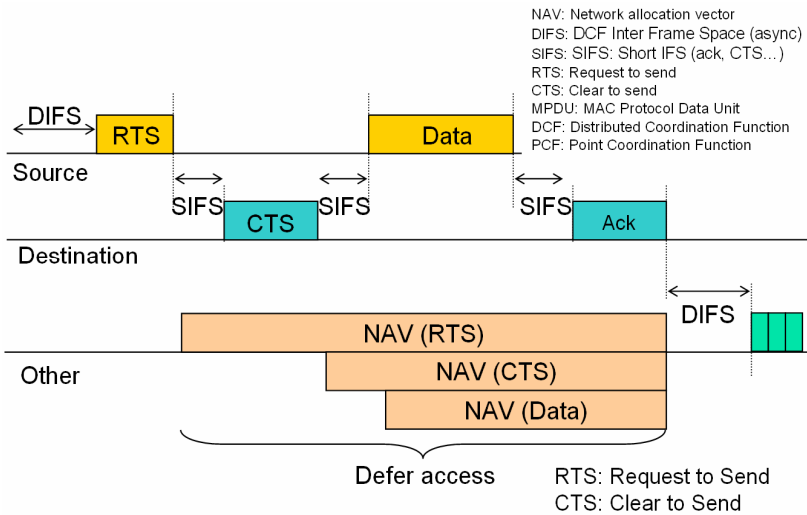
** Corresponding author.

time using NAV and Master measures the network congestion. And then according to the measured value, deadlock state is defined to stop data transmission for a certain period and prevent system resource and energy consumption from wasting. In addition, the purpose of UWA-NAV is diverse. It can be used for Master's data transmission, network reconfiguration, new nodes' joining with network and etc. NAV is used to prevent system resource, such as energy and bandwidth, from wasting and stops all data transmission for a certain period. In this paper, by using UW-NAV technique, a method, which is adaptive to rapidly fluctuating transmission failure rate, was proposed for reducing energy consumption.

The structure of this paper is as follows. In Chapter 2, NAV technique of IEEE 802.11x is briefly reviewed. In Chapter 3, the proposed UWA-NAV technique is described in details. In Chapter 4, the performance of the proposed method is analyzed. Lastly conclusions are in Chapter 5.

2 NAV in IEEE 802.11x [1][2]

The Network Allocation Vector (NAV) is a method to avoid collisions in a shared transmission medium.



(A. Leon-Garcia, I. Widjaja, Communication Networks, Instructor's Slide Set)

Fig. 1. NAV Operation

Each station wishing to transmit through the shared medium performs a RTS with a NAV that indicates the time required to complete the wished transmission. If no collision is detected and after the acknowledge published by the receiving station in a

CTS packet, every connected station consider the shared medium allocated to the sending station during the time specified in the NAV. This technique is used within IEEE 802.11 (Wi-Fi) and IEEE 802.16 (WiMax) networks [3].

3 NAV and Congestion Control in Underwater Communication

3.1 Underwater Acoustic Sensor Network (UW-ASN) MAC Mechanism

In this section, several presuppositions with brief descriptions of MAC design were mentioned. (Author has been studying MAC systems for UW-ASN). Firstly, the proposed MAC system is for monitoring sea environment with 2D topology of cluster-type. No moving object (AUV) is considered and TDMA (Time Division Multiple Access) is adopted for communication between clusters. Nodes will transmit data periodically according to the pre-defined schedule. The system has 5 steps for its communication

- 1) *Network Initiation and configuration (CH+SNs)*
- 2) *Broadcast to all member node with Acks(CH)*
- 3) *Data transmission (SNs)*
- 4) *Repeat 2) ~ 3) step*
- 5) *Network reconfiguration (CH+SNs)*

More detailed explanation and system spec can be found in [4] and [5].

3.2 UWA-NAV

In this section, a new definition of UWA-NAV and its procedure were explained. The necessity of UWA-NAV depends on the sea environment. Since Acoustic is used for communication, there are many sources of artificial and natural noise such as low frequency sounds generated by ships and machines, high frequency sounds generated by dolphins. The sources and their effects are Seismo-acoustic noise, Shipping noise, Bio-acoustic noise, Wind and rain noise, Depth dependence, Directionality, Arctic ambient noise, Acoustic daylight and etc. For last 3 decades, many researchers have conducted various tests and modeling works to make better noise model[6]. The latest version of numerical noise model (RANDI III – The research ambient-noise directionality III) was developed for application to shallow-water and coastal areas in the low-to-mid frequency range (~10-300Hz)[6]. The receiver can be either a horizontal or a vertical line array (Breeding, 1993). However, no unified model considering various sea environments was proposed yet and still it remains as a challenging research area [6].

Firstly, UWA-NAV is handled by CH. CH is a scheduler for unit network and controls TDMA scheduling, various guard band settings, Ack transmission, Power saving mode controls and etc. It also controls the waste of the energy resource using UWA-NAV flag. When the transmission rate of the network is remarkably decreased or error rate is rapidly increased, CH can calculate the trade-off relationship between

the transmission efficiency and the energy consumption rate by measuring SNR or referring LQI information. In case of conducting non transmission mode according to a certain policy based on pre-defined threshold value, devices can prevent the waste of network resource and energy consumption resulted from significantly increased transmission failure rate by maintaining power saving mode and stopping data transmission during a certain period. However, as for the number of packets which are succeeded in transmission, the conventional method can process more packets than the proposed method. Based on the fact that if error rate gets higher than a certain level then the success rate of packet transmission increases rapidly, the proposed method can be a scheme preventing serious waste of network resource [4].

3.3 UWA-NAV Flag

Figure 2 shows an example of frame format for values of UWA-NAV included and transmitted with Control (Beacon) Packets.

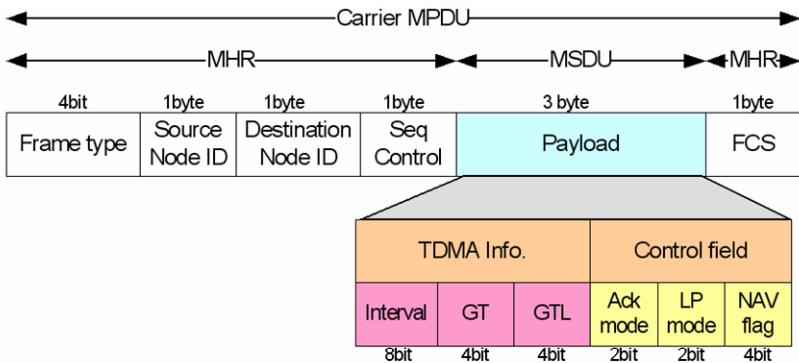


Fig. 2. An Example of Control (Beacon) Frame with NAV flag

Table 1. An Example of NAV flag

| | | | |
|------------------|-----------------------|-----------|--|
| NAV Flag (4bits) | Non transmission mode | 0000 | 1 Level Deadlock state for error control |
| | | 0001 | 2 Level Deadlock state for error control |
| | | 0010 | 3 Level Deadlock state for error control |
| | | 0011 | 4 Level Deadlock state for error control |
| | | 0100 | 5 Level Deadlock state for error control |
| | | 0101 | 6 Level Deadlock state for error control |
| | | 0110 | 7 Level Deadlock state for error control |
| | | 0111 | 8 Level Deadlock state for error control |
| | Transmission mode | 1000~1111 | Reserved |

NAV flag of 4 bits included in Control field can operate in Non transmission mode as shown in the table below. 8 steps of adaptive error controls are possible and NAV duration time is also controllable according to its error rate. Threshold value can be adjusted by a system manager and the required field among 1~8 steps can be specified taking various environmental condition into consideration.

3.3 NAV Flag Generation Procedure

For the calculation of NAV flag, the measurement of SNR (or LQI) value and delay time of network has to be done. The delay time can be measured together with the propagation delay by using the information of time stamp of network initiation and data transmission. SNR and LQI are values for measurement of error rate which has been typically used in sensor network system. At this time, since a policy table of user defined UWA-NAV already exists, the final NAV flag can be set-up.

Figure 3 shows the conceptual diagram of NAV flag generation procedure.

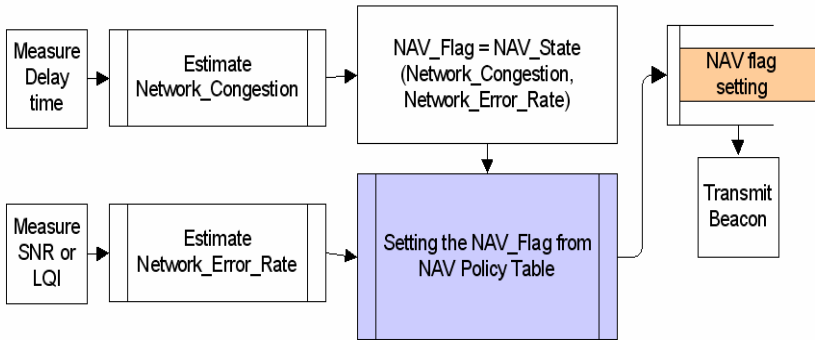


Fig. 3. NAV flag Generation Procedure (CH side)

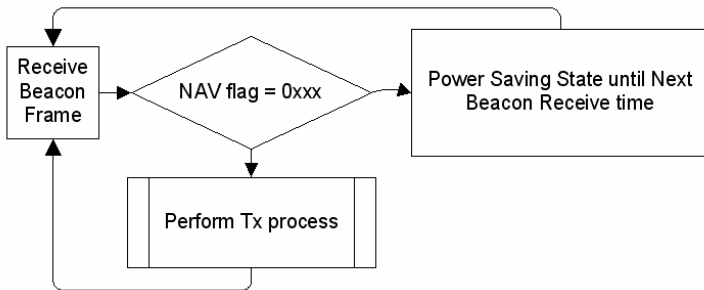


Fig. 4. UWA-NAV Transmission Procedure (sensor node side)

After CH transmits NAV flag which is included in Beacon frame, the sensor node, which is located in the receiving cluster, stops transmitting for a certain time according to the types of NAV policy table and maintains power saving mode until the next receiving of Beacon frame. And the sensor node repeats the same procedure until the newly received NAV flag of Beacon frame is changed and the network communication is re-opened again. Figure 4 shows the brief procedure seen from the sensor node side.

4 Simulation Result

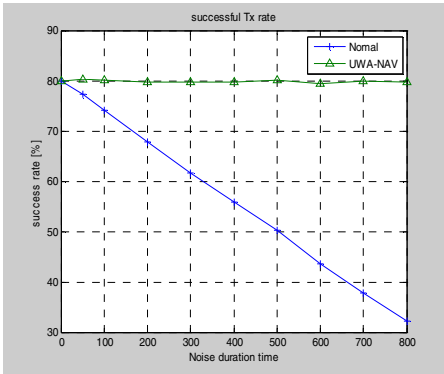
In this paper, a moving ship is assumed as a constant noise source and a periodic data acquisition in shallow water by the network is assumed. This system presupposes the situation of receiving sea environment monitoring data from sensor nodes and transmitting the data to BS (surface). Transmission failure and the waste of network resource caused by very high error rate are compared from the point of energy consumption. Table 2 shows the parameters for the performance comparison.

Table 2. Simulation parameters

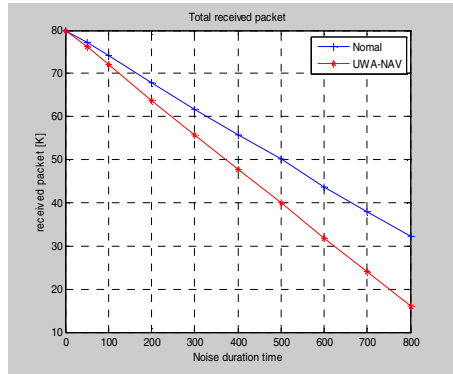
| Parameters | Values |
|------------------------------|------------------------------------|
| Simulation time | 1,000 Sec |
| Data transmission | 100 packets / sec |
| Noise duration time | 50 ~ 800 Sec |
| Error reduction rate | 30% |
| Fluctuation of error rate | 50% |
| Noise Source | A vessel |
| Energy exhaustion unit (EEU) | 1 (per 100 transmit + 100 receive) |
| Default error rate | $10^{-1} \sim 2 \times 10^{-1}$ |

10 steps of the noise duration times are generated and the performance is calculated and analyzed. Figure 5 shows the success rate of transmission-trying packets (Figure 5(a)), transmission rate of overall network (Figure 5(b)), energy consumption of the network (Figure 5(c)) and the energy efficiency (Figure 5(d)).

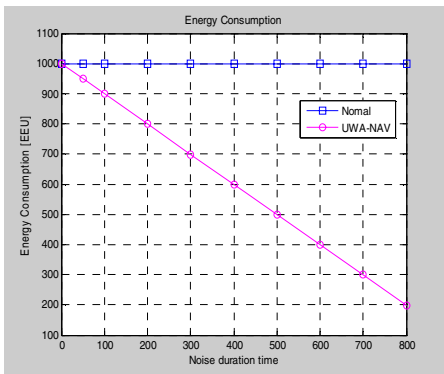
In case that the system processing rate decreases rapidly by constant occurrence of transmission error and the transmission is prevented by the value of UWA-NAV, the transmission efficiency is improved as the noise duration time increases comparing with normal case. It is because the number of total Tx/Rx done packets increased although the success rate is small.



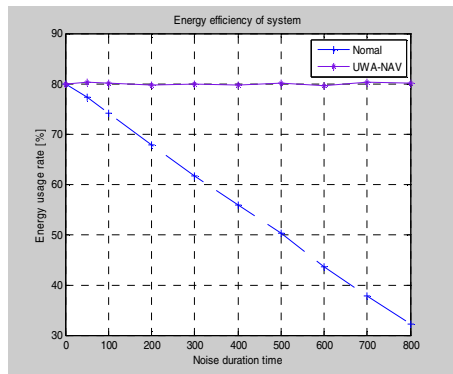
(a) Successful Tx rate



(b) Total Tx/Rx done packet



(c) Energy consumption



(d) Energy efficiency of system

Fig. 5. Simulation results

5 Conclusion

In this paper, a method for reducing the waste of system resources and energy consumption was proposed. The proposed method occupies transmission period by using UWA-NAV and the network congestion is measured by Master. Based on the measured values, Deadlock state is set up to stop data transmission to improve system’s resource usage and its energy efficiency. Simulations were conducted to verify the performance of the proposed method which is adaptive to severe fluctuation of the transmission failure rate caused by constant noise source in underwater network environment.

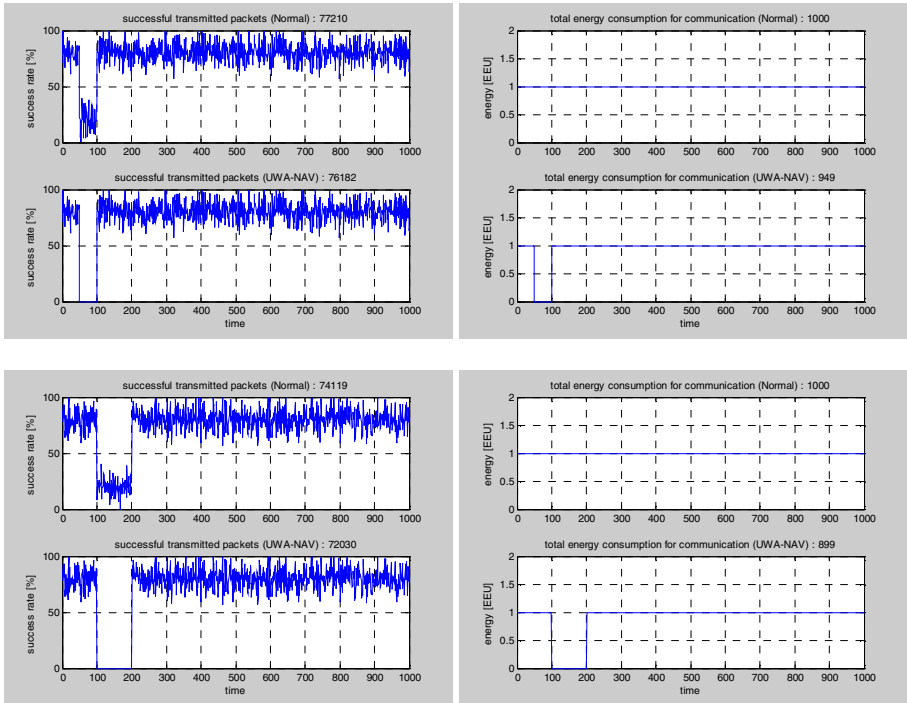
UWA-NAV is not adequate to real time data transmission which has a limitation of transmission times. It is because that, during noise generating period, time delay is caused and there can be data without change of transmission trial in case of not enough carrying queue in the system. It is expected that these problems can be solved by aggregation technique and fitter. Further study for ensuring data transmission reliability and transmission mode of UWA-NAV is planned.

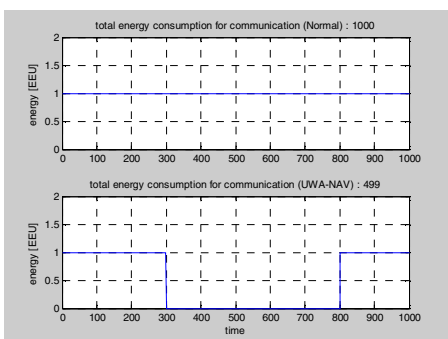
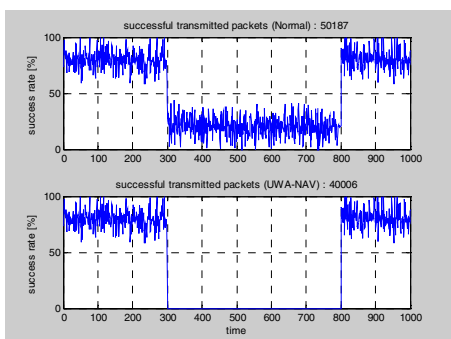
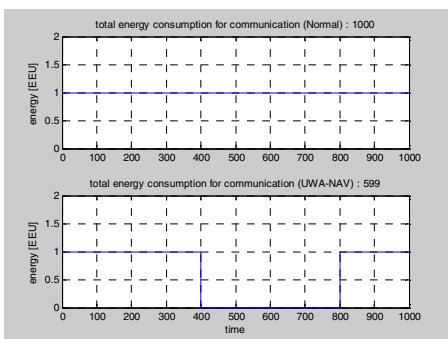
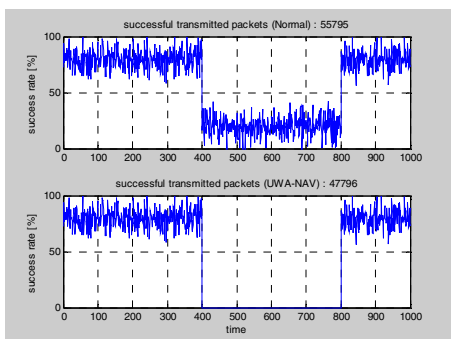
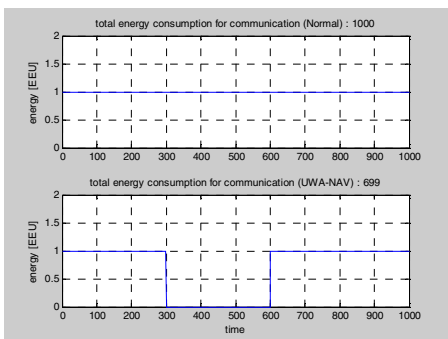
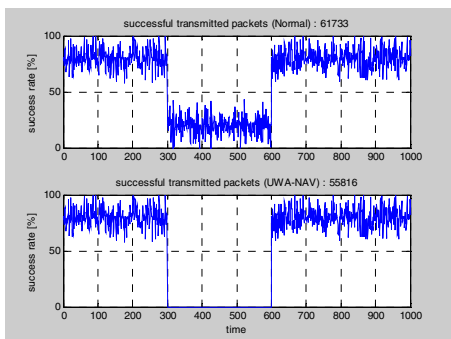
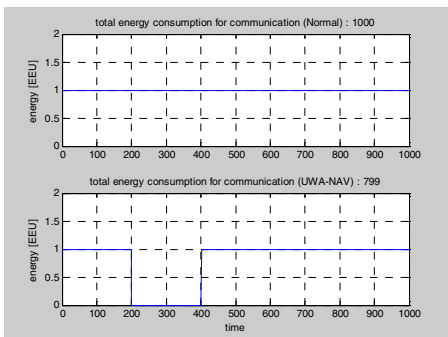
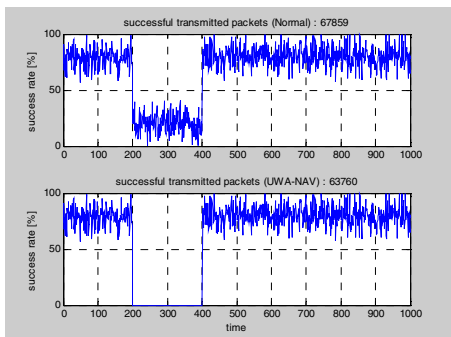
References

- [1] Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: higher speed physical layer (PHY) extension in the 2.4GHz band, IEEE Std 802.11b (April 1999)
- [2] IEEE Standard 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003) (2005)
- [3] Liu, H.-H., Wu, J.-L.C., Chen, W.-Y.: New frame-based network allocation vector for 802.11b multirate wireless LANs, Communications. IEE Proceedings 149(3), 147–151 (2002)
- [4] Shin, S.Y.: Smart Blocking Media Access Control Mechanism for UW-ASN, Thesis for the Degree of Ph. D, Kookmin Univ. (January 2007)
- [5] Shin, S.Y., Choi, J.K., Park, S.H.: Transmission Environment for Underwater Acoustic Communication. In: ITPA 2007 (September 2007) (will be published)
- [6] Paul, C.: Underwater Acoustic Modeling and Simulation. Spon Press, London (2003)

Appendix

We classified the transmission environment into 9 cases. Figure 6 shows the simulation results of noise duration time ranging from 50 to 800 seconds. The left figure shows the real time transmission success rate in percentage and the right one represents the energy consumption value (EEU).





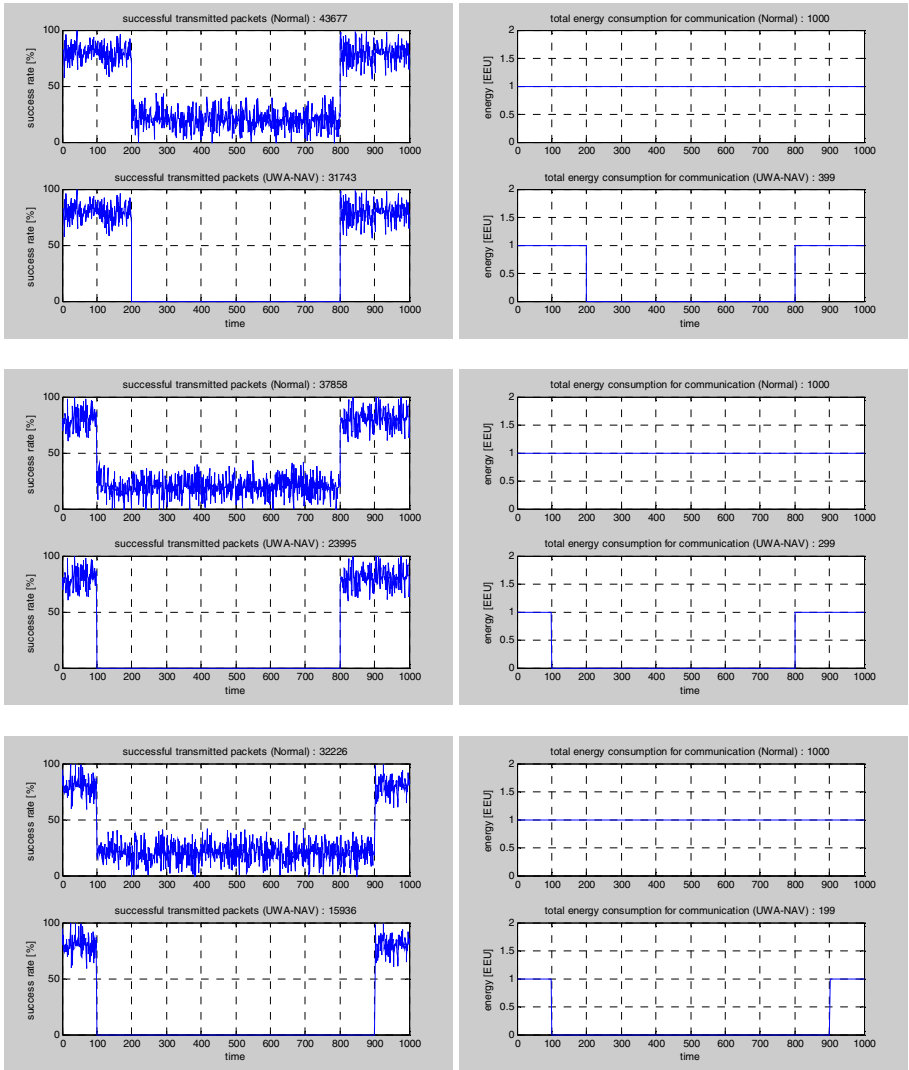


Fig. 6. Tx/Rx packets and Energy consumption (Noise duration time: 50~800 sec)

Underwater Wideband Source Localization Using the Interference Pattern Matching

Seung-Yong Chun¹, Se-Young Kim², and Ki-Man Kim²

¹ Agency for Defense Development,
#1 Hyun-dong, 645-016 Jinhae, Korea
ddoyong@dreamwiz.com

² Dept. of Radio Communication Eng., Korea Maritime University,
#1 Dongsam-dong, Yeongdo-ku, 606-791 Busan, Korea
sgtgfm@hhu.ac.kr, kimkim@hhu.ac.kr

Abstract. Recently many studies have been performed to detect underwater target by sensor network. This paper proposes an underwater source localization method based on wideband interference pattern matching. Matching of two interference patterns which seen in the sensor spectrograms, estimates a ratio of the range from source to two sensors according to the waveguide invariant theory and this ratio applied to circle of Apollonius. The circle of Apollonius is defined as the locus of all points whose distances from two fixed points are in a constant ratio so it is possible to represent the locus of potential source location. However, since ambiguity of absolute source location so it requires that additional equation which estimates another locus of the source. Therefore the hyperbola equation by estimating TDOA (Time Difference Of Arrival) is introduced into localization and finally cross point of two equations can be estimated as the source location. We performed simulation to test performance of the proposed localization method and then practiced error analysis of the results. And we tested performance of capability from a real-data collected during sea experiment. From simulation and experimental results, proposed algorithm represents that estimated position of target showed error of within 10%.

Keywords: source localization, waveguide invariant, IPM (Interference Pattern Matching), circle of Apollonius, hyperbola equation.

1 Introduction

Source localization in shallow water has been considered many times over the past years and many studies have been achieved in order to improve the performance. In shallow water environment, complicated phenomenon such as multipath propagation and beam spreading degrades the performance of estimates the source. Conventional plane-wave beamforming and MUSIC (MULTiple SIGNAL Classification) have been discussed general localization techniques. However these techniques dose not

sufficiently consider that the propagation characteristics in ocean waveguide therefore in the real ocean their performance reduce with large localization error.

For this reason there are several attempts have been made to localize for a long range source by exploiting multi-modal dispersion such as MFP(Matched Field Processing) technique based on acoustic propagation model in multi-path environment[1], and recent array invariant theory derived by S.W. Lee[2].

In particular a study on localization technique using waveguide invariant theory has been attained. The range of the source can sometimes also be estimated by the much simpler waveguide invariant theory. The invariant parameter called β is useful for describing the characteristic of the acoustic waveguide. However the waveguide invariant method requires knowledge of certain “invariant” parameter β which unfortunately often vary with sound speed structure of the ocean. Recently several methods are introduced using the waveguide invariant theory and showed enhanced performance. But they are still dependent on the β and ocean environment. So it is necessary to localize the source that independent of the β without the information of the ocean environment. Therefore in this paper, we propose a source localization method that has advantages of not regard for β and much simpler.

2 Waveguide Invariant and Interference Pattern

Interference pattern which seen in the sensor spectrograms collected from the moving ship-radiated noise arise from the mutual interference between modes reflected by the surface and the bottom. The slope of the interference pattern has been known invariant. Waveguide invariant parameter, designated as β , has been known that a slope of the interference pattern is directly proportional to the range of the source [3].

The β is approximately 1 in the Pekeris waveguide however in the case of the real ocean the β is variable with mode number, frequency and source depth, so knowledge of a certain invariant parameter is necessary to source localization.

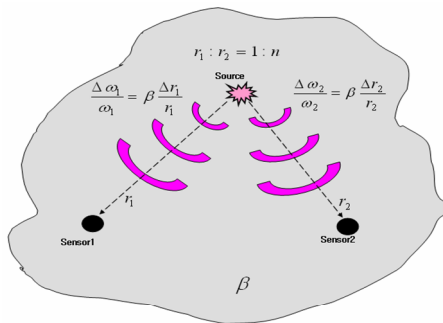


Fig. 1. The characteristic of waveguide invariant in identical pressure field

If two sensors are used to source localization in identical acoustic propagation environment it is possible to detect the source without regard for β because of the β has identically effect on the each sensor. Figure 1 shows that the characteristics of waveguide invariant for two sensors which are located in identical pressure field.

The relationship between β and slope of the interference pattern for each sensor can be expressed as

$$\begin{aligned} \frac{d\omega/\omega}{dr/r} &= \left(\frac{k_m - k_n}{\omega} \right) / \left(\frac{dk_m}{d\omega} - \frac{dk_n}{d\omega} \right) \\ &= - \left(\frac{1}{v_m} - \frac{1}{v_n} \right) / \left(\frac{1}{u_m} - \frac{1}{u_n} \right) \equiv \beta_{mn} \end{aligned} \quad (1)$$

Here k_m and k_n are m th and n th mode wave number as a function of the frequency respectively, $v_m = \omega/k_m$ and $v_n = \omega/k_n$ are m th and n th phase velocity respectively, $u_m = d\omega/dk_m$ and $u_n = d\omega/dk_n$ are m th and n th group velocity respectively. Equation (1) summarized as follows

$$\begin{aligned} \frac{d\omega_1}{\omega_1} &= \beta \frac{dr_1}{r_1} \\ \frac{d\omega_2}{\omega_2} &= \beta \frac{dr_2}{r_2} \end{aligned} \quad (2)$$

r_1 and ω_1 are the range from the source to sensor 1 and frequency of the interference pattern in spectrogram for sensor 1, respectively. r_2 and ω_2 are the range from the source to sensor 2 and frequency of interference pattern in spectrogram for sensor 2, respectively. Since β has identically effect on the each sensor equation (2) summarized as

$$\frac{r_1}{r_2} \frac{\omega_2}{\omega_1} = \frac{dr_1}{dr_2} \frac{d\omega_2}{d\omega_1} \quad (3)$$

Assuming that $r_1 = nr_2$ where n is ratio of the range from source to two sensors, one finds

$$n = \frac{r_2}{r_1} = \frac{\omega_2}{\omega_1} \quad (4)$$

From equation (4) it is notice that the ratio of frequency same as the ratio of range. Consequently ratio of the frequency between interference patterns which seen in each single sensor spectrogram, represents a ratio of range between source and each sensor.

3 Proposed Algorithm

3.1 Interference Pattern Matching (IPM)

The ratio of the range between source and two sensors is estimated by interference pattern matching (IPM). Figure 2 shows a process of the IPM. Sensor 1 is selected reference spectrum and the spectrum of sensor 2 scaled until matched spectrum of sensor 1. If the RMSE (Root Mean Square Error) between sensor 1 spectrum and scaled sensor 2 spectrum is the most smaller then the ratio of scale can be estimated as the ratio of range.

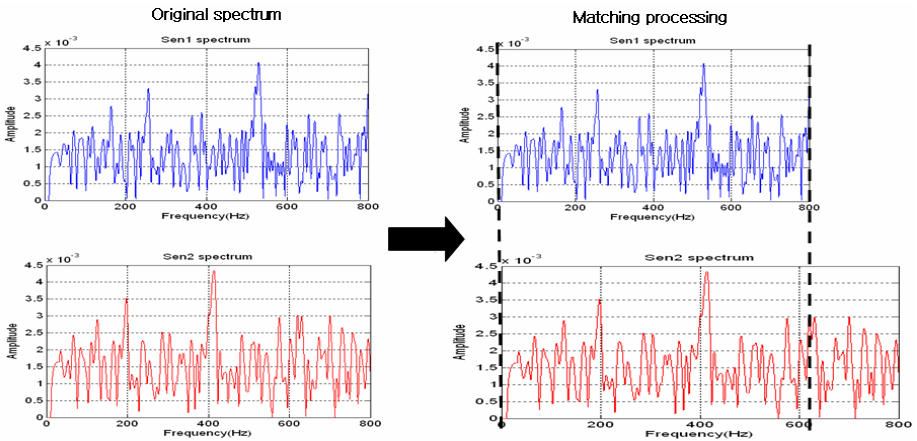


Fig. 2. Interference pattern matching process

Estimated ratio of range applied to circle of Apollonius. Circle of Apollonius shown in Figure 3 defined as the locus of a point whose distance from a fixed point is a multiple of its distance from another fixed point. If the multiple is equal to 1, then the locus is a line which is perpendicular bisector of the segment of each fixed point and the multiple is not equal to 1, then it is a circle so called circle of Apollonius [6].

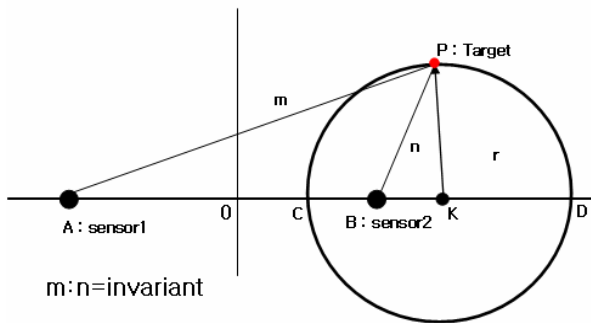


Fig. 3. Circle of Apollonius

3.2 Source Localization by Two Equations

The result from IPM estimates the locus of the source using the circle equation derived from the principal of the circle of Apollonius. But it requires other equation in order to estimate the absolute source position because the circle equation can make only one of locus in the case of two sensors. So the second relative range between source and two sensors is estimated by introducing TDOA (Time Difference Of Arrival) technique [7]. The estimated TDOA between two sensors is applied to hyperbola equation. Finally cross point of the circle and hyperbola can be estimated as the position of the source. Figure 4 shows the interaction point of the circle of Apollonius and hyperbola.

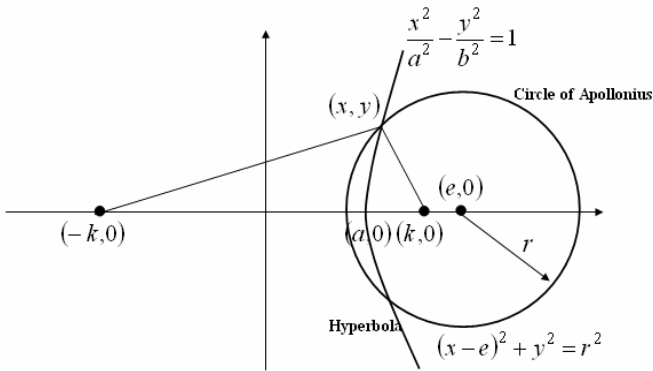


Fig. 4. Interaction point of the circle of Apollonius and hyperbola

The corresponding with coordinates of the source can be expressed as following solutions of two equations.

$$x = \frac{a^2 k + a \sqrt{a^2 k^2 - (a^2 + b^2)(k^2 - b^2 - r^2)}}{a^2 + b^2} \quad (4)$$

$$y = \pm \sqrt{\frac{b^2}{a^2} k^2 - b^2}, \text{ if } x^2 > a^2$$

4 Simulation and Experimental Results

We performed simulation of 3 scenarios to test the IPM algorithm and proposed localization method and then practiced error analysis of the results. And we tested performance of a real-data collected during MAPLE-05 experiment applied to the proposed algorithm.

4.1 Simulation Results

We demonstrate the performance of the proposed localization algorithm with simulated pressure field based on KRAKEN normal mode program [8]. Figure 5 shows the three cases for the simulation.

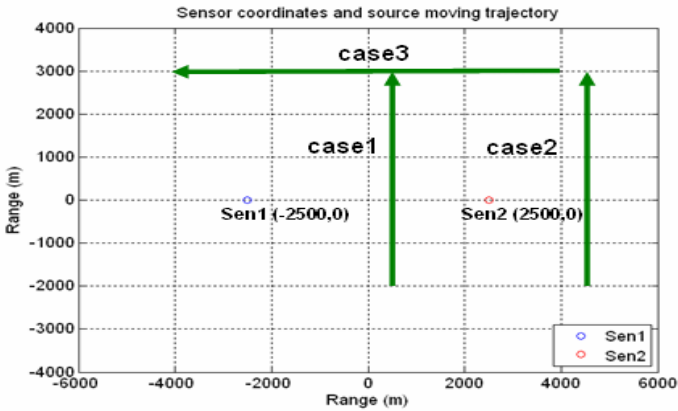


Fig. 5. Three cases for the simulation

The distance of each sensor is 5 km. The speed of moving target is 5 knot and range of trajectory is 5 km during about 32 minutes for case1 and case 2. In case 3 range of trajectory is 8 km during about 51 minutes. Target signal has 1 to 800 Hz band. The source localization performed at intervals of 250 m in trajectory and the results of error for simulation are presented at table 1.

Table 1. Results of error in simulation

| | IPM error | Mean tracking error(m) | Mean tracking error rates (%) |
|-------|-----------|------------------------|-------------------------------|
| Case1 | 0.0031 | 47.37 | 4.14 |
| Case2 | 0.1787 | 210.87 | 4.39 |
| Case3 | 0.0133 | 96.91 | 2.46 |

From table 1, the proposed algorithm based on IPM seemed to have excellent performance whose mean tracking error rates is within 5%, but if examine a RMSE (Roots Mean Square Error) pattern according to the adjust IPM ratio, it showed the minimum value even in error point. We conclude this is due to the sensor spectrum adjusted linearly without previous knowledge of environment on β and environmental parameter of the real ocean. In particular results of case 2 represent a great tracking

error proportional to IPM error. So in order to improve the performance it is necessary to estimate correct ratio of IPM.

4.2 Experimental Results

The source tracking result for experiment demonstrated at figure 6. The speed of moving target is 4 knot and the distance of each sensor is 66 m. Target signal has 1 to 400 Hz band. From the result though it is note that a little difference between true position and estimated position but tracking tend to true trajectory.

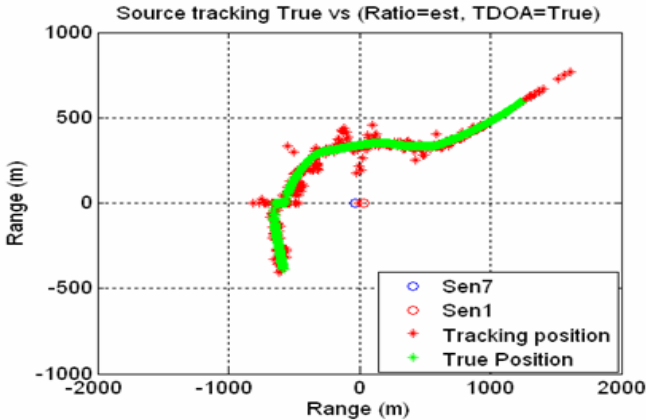


Fig. 6. Source tracking result for MAPLE 05 experiment

If examine the experimental result, since the estimated position of target showed error of within 10%, so proposed algorithm is even available in real ocean. The IPM proposed in this paper and localization method with TDOA are possible to be applied to identical pressure field without regard for β , and need no previous knowledge of environment. Also, because only two sensors make localization possible, this is expected to adapt sufficiently to the field of active sonar and passive sonar using property of broadband signal.

5 Conclusions

The localization method based on IPM has been introduced for estimates source position without regard for β and knowledge of the ocean environment. It has been shown that proposed method does not require extensive computations because only two equations are used. The ability to make simple and accurate source tracking by the proposed method has been demonstrated with simulation and real data from the MAPLE 05. In future work, it is needs to test the performance in range dependent environment and the research of 3-D source localization.

References

1. Baggeroer, A.B., Kuperman, W.A., Schmidt, H.: Matched field processing: source localization in correlated as an optimum parameter estimation problem. *J. Acoust. Soc. Am.* 83, 571–587 (1988)
2. Lee, S.W., Makis, N.C.: The array invariant. *J. Acoust. Soc. Am.* 119(1), 336–351 (2006)
3. D’Spain, G.L., Kuperman, W.A.: Application of waveguide invariants to analysis of spectrograms from shallow environments that vary in range and azimuth. *J. Acoust. Soc. Am.* 106(5), 2454–2468 (1999)
4. Brekhovskikh, L.M., Lysanov, Y.: *Fundamentals of Ocean Acoustics*, 3rd edn. Springer, Heidelberg (2003)
5. Jensen, F.B., Kuperman, W.A., Porter, M.B., Schmidt, H.: *Computational Ocean Acoustics*. AIP, New York (1994)
6. Georgia University dept. of mathematics education, <http://jwilson.coe.uga.edu>
7. Fertner, A., Sjolund, A.: Comparison of various time delay estimation methods by computer simulation. *IEEE Trans. Acoust. Speech Signal Process.* ASSP-34(5), 1329–1330 (1986)
8. Porter, M.B.: The KRAKEN Normal Mode program, SACLANT Undersea Research Centre (1994)

A New Virtual Select Database Operation for Wireless Sensor Networks

Seungjae Lee*, Changhwa Kim, and Sangkyung Kim

Department of Computer Science and Engineering
Kangnung National University
Jibyun-dong, Gangnung-si, Gangwon-do
Korea
{silveree*, kch, skkim98}@kangnung.ac.kr

Abstract. Sensor networks gather tremendous data from some wide range of area and databases are good to process and manage such tremendous data. However, there might happen some problems on applying database concepts into wireless sensor networks. The reason is because from the viewpoint of wireless sensor networks, situations under which some operations should be performed on non-existing data may occur frequently. For instance, consider the following examples: How can we write a query to get the locations at which the temperature is 22°C, given a sensor network area in which there are some spots at exactly 22°C but there is no sensor node to announce exactly 22°C? Can we write a query to get the temperature of a spot with no sensor node? In order to solve the above described problems, we propose the new database operation for sensor networks and show how the above queries' results could be obtained using this new operation. This new database operation can provide more effective data management and standard interfaces to application programs for sensor networks. Furthermore, it is also helpful to save a node's energy by reducing the number of communications for processing a query and enhances the robustness of a sensor network system.

Keywords: database, select operation, communication energy, wireless sensor network.

1 Introduction

As implementation areas of wireless sensor networks become wider, more research is being done on relational database approaches to wireless sensor networks in order to process and manage tremendous amount of sensing data which is being gathered. However, there might be some problems in directly applying traditional relational database concepts into a wireless sensor network [1,4,5].

Assuming a temperature monitoring wireless sensor network in which temperature sensor nodes are scattered randomly, each node can be described as a point in the whole network area and nodes cannot cover the whole network area continuously. In this situation, if one poses a query to determine the temperature of a point where no

sensor node exists, the result would be an empty set because there is no tuple related to the location. And if he or she poses a query to determine locations with 22°C, the result would be an empty set or few tuples because only sensor nodes which sense exactly 22°C would respond.

The virtual select operation, proposed in this paper, is an operation which can generate non-existing tuples, called to virtual tuples, in the relation. This operation extracts the tuples from the relation if there are tuples that are satisfied with the predicate of the operation in the relation. But if there is no such tuple that satisfies the predicate, the operation generates virtual tuples with real existing tuples, called to the source tuples, of the relation. Generated virtual tuples are tuples created with estimated attribute values by the virtual select operation that could not be generated by combining tuples in the relation or by any other traditional database operations.

Applying a relational database with the virtual select operation, we can pose a query more freely. It enables application code simpler and can provide standard application interfaces. Moreover, it also enables to save node's transmission energy which is a very important research topic on wireless sensor networks. In underwater acoustic sensor networks, energy constraint is more important because acoustic waves need more transmission energy than radio waves and batteries are hard to be recharged or replaced.

The rest of this paper is structured as follows. In Section 2, we present a brief overview of the related works and Section 3 describes the virtual select operator in detail. Section 4 describes how to apply this new operation to wireless sensor networks and the performance analysis is shown in Section 5. Finally, Section 6 concludes and finalizes this paper.

2 Related Works

In a wireless sensor network, database concepts, especially relational database, are used in order to manage tremendous amounts of data effectively. A wireless sensor network can be regarded as a database called to a wireless sensor network database. A tuple, in a wireless sensor network database, is configured with a sensing value, a sensing time, a node's location, etc. A set of sensing values gathered from a class of sensor nodes is treated as an attribute and a set of tuples created by a class of sensor nodes is treated as a relation [1].

On materializing a wireless sensor network database, some work has shown that in-network processing of sensor data is fundamental to achieving energy-efficient communication in wireless sensor networks [1,2,3].

For those who continuously monitor the environment, approximate answers have another feature, called streamed results, that is important for wireless sensor networks. Users can get partial query results and dynamically refine their queries with this feature. This capability, called online aggregation, has been proposed in database literature for large on-line decision support systems. In the wireless sensor network context, users could approach more specific queries [6,7,8].

3 Virtual Select Operation

The virtual select operation generates virtual tuples with existing tuples in a relation. We use σ^v to denote the virtual select operation which is similar with the symbol of select operation in relational algebra. All basis attributes must be appeared in operator's predicate.

The basis attribute values of virtual tuples to be created are defined at predicate of the virtual select operation and can be constant values or ranges. If B_1 is a basis attribute and c_1 and c_1' are constants, constant predicate is declared to be. In the case of range predicate, five types are available like $c_1 \leq B_1 \leq c_1'$, $B_1 \leq c_1$, $B_1 \geq c_1$, $B_1 : c_1$ and $B_1 \neq c_1$. $B_1 : c_1$ means $(-\infty, \infty)$. c_1 is called the origin value which is the basic attribute value to create virtual tuples and is explained below in detail.

We call these six predicate types standard predicate types. A virtual select operation with range predicate can be converted into union of virtual select operations with constant predicate.

Predicate in a virtual select operation must have terms on all basis attributes. Predicate which is expressed as logical AND(\wedge) for standard predicate is called to normalized predicate and a virtual select operation expressed as non-normalized predicate can be converted into union of virtual select operation expressed as normalized predicate.

The virtual select operation is expressed as (1) with normalized predicate

$$\sigma_{P_1 \wedge P_2 \dots \wedge P_\beta}^v (relation) \tag{1}$$

where

$$P_i \begin{cases} B_i = c_i \\ c_i \leq B_i \leq c_i' \\ B_i \leq c_i \\ B_i \geq c_i \\ B_i : c_i \\ B_i \neq c_i \end{cases} \quad c_i, c_i' : \text{constants}, 1 \leq i \leq \beta$$

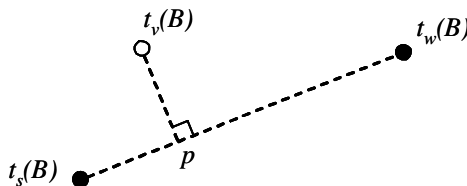


Fig. 1. Tuple vectors in Euclidean b-space

Only tuples in which the distance between the tuple vector of the virtual tuple for the basis attribute set B and that of itself is under θ can be source tuples.

A method to calculate the estimate attribute values is like below.

Let $t_s(B)$ and $t_w(B)$ be source tuples for a virtual tuple $t_v(B)$. Then tuple vector vectors of $t_s(B)$, $t_w(B)$ and $t_v(B)$ are described in Euclidean b-space and p is a point where $\overline{t_s(B)t_w(B)}$ and $t_v(B)$ crosses at right angles like figure 1.

Then assuming that the ration of $\left| \overline{t_s(B)p} \right|$ and $\left| \overline{t_s(B)t_w(B)} \right|$ is the same as that of $\left| t_s.e_j - t_v.e_j \right|$ and $\left| t_s.e_j - t_w.e_j \right|$ for all $1 \leq j \leq \mathcal{E}$ where \mathcal{E} is the number of estimate attributes, we can calculate estimate attribute values $t_v.e_j$ using (2).

$$\left| \overline{t_s(B)p} \right| : \left| \overline{t_s(B)t_w(B)} \right| = \left| t_s.e_j - t_v.e_j \right| : \left| t_s.e_j - t_w.e_j \right| \tag{2}$$

As $\left| \overline{t_s(B)p} \right| = \frac{\overline{t_s(B)t_v(B)} \bullet \overline{t_s(B)t_w(B)}}{\left| \overline{t_s(B)t_w(B)} \right|}$, we can write $t_v.e_j$ as (3).

$$t_v.e_j = t_s.e_j - \frac{(t_s.e_j - t_w.e_j) \{ (t_v(B) - t_s(B)) \bullet (t_w(B) - t_s(B)) \}}{\left| t_s(B) - t_w(B) \right|^2} \tag{3}$$

Therefore, t_v can be written as (4). If there are more t_s or t_w that satisfy the threshold condition, it iterates the above procedure to create all possible virtual tuples.

$$t_v = (c_1, c_2, \dots, c_b,$$

$$\begin{aligned} & t_s.e_1 - \frac{(t_s.e_1 - t_w.e_1) \{ (t_v(B) - t_s(B)) \bullet (t_w(B) - t_s(B)) \}}{\left| t_s(B) - t_w(B) \right|^2}, \\ & t_s.e_2 - \frac{(t_s.e_2 - t_w.e_2) \{ (t_v(B) - t_s(B)) \bullet (t_w(B) - t_s(B)) \}}{\left| t_s(B) - t_w(B) \right|^2}, \\ & \vdots \\ & t_s.e_{\mathcal{E}} - \frac{(t_s.e_{\mathcal{E}} - t_w.e_{\mathcal{E}}) \{ (t_v(B) - t_s(B)) \bullet (t_w(B) - t_s(B)) \}}{\left| t_s(B) - t_w(B) \right|^2} \end{aligned} \tag{4}$$

4 Implementing Virtual Select Operation on Wireless Sensor Networks

To perform virtual select operation at sensor nodes, it requires two conditions to be satisfied, which are generally valid in wireless sensor networks:

- Each sensor node can communicate directly with nearby nodes.
- The distance between inter-source tuple pairs is less than the transmission range of sensor nodes.

When a sensor node receives a query, it checks whether or not it satisfies predicate itself. If satisfied, it sends a tuple using its own data and finishes the query. Otherwise, it broadcasts the tuple to nearby sensor nodes to create a virtual tuple.

To receive tuples from nearby nodes, it would wait for some brief time which would be stored in the information base of a query layer.

After a sensor node receives tuples from nearby nodes, it checks whether its basis attribute values are the same as those of the received tuple or not. If all basis attribute values are the same, it discards a received tuple. If any of the values is not the same, the node determines whether or not it is the strong sensor node.

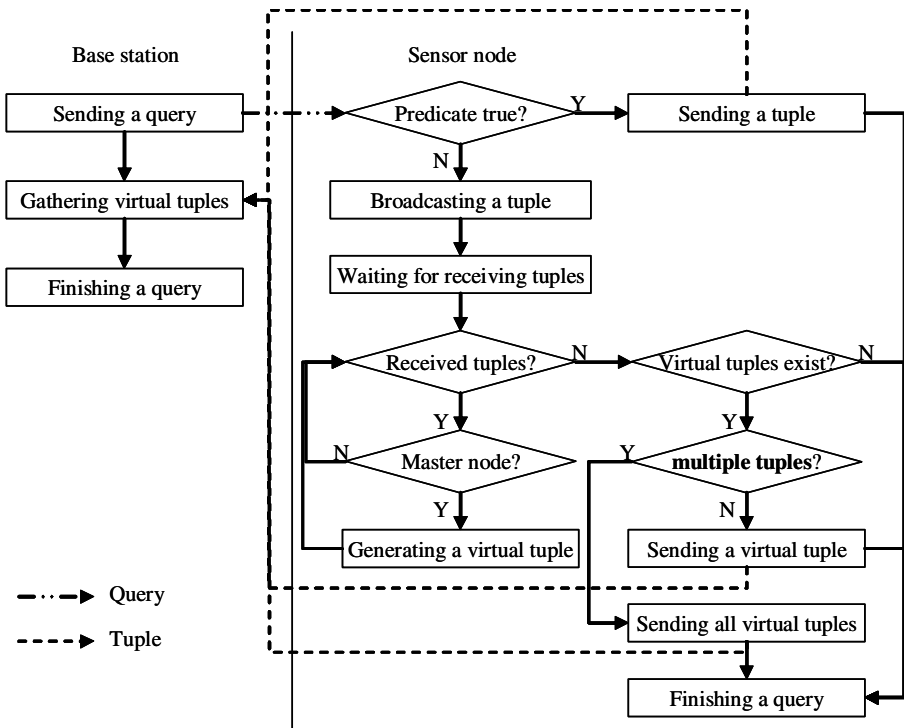


Fig. 2. A process diagram of a virtual select operation

A sensor node which provides a strong tuple is called to a strong sensor node and the other sensor node which provides a weak tuple is called the weak sensor node. If two tuples t_1 and t_2 can be a strong tuple at the same time, it is determined by attribute values of the basis attribute set B . Using $t_1(B) \neq t_2(B)$, by definition of a strong and weak tuple, we choose i that satisfies $t_1.b_i \neq t_2.b_i$ at the first time as increasing i from 1 to β and determine the tuple that has the larger b_i as the strong tuple. A strong node might be a master node that generates and sends a virtual tuple.

However, if each node knows its hop count from its own location to the base station, it would be ideal for the sensor node which has the shorter hop count to be a master node. To do this, each node should broadcast its hop count along with its tuple.

If the sensor node is determined not to be a master node, it discards the received tuple. A master node configures a virtual sensor node using data from itself and the other sensor node which sent the tuple. And it also evaluates whether or not the source tuple pair is valid for constraints of θ . If this is not a valid pair, it discards the source tuple pair. If it is a valid pair, a master node generates and sends a virtual tuple to the base station.

Figure 2 illustrates these processes with a diagram.

5 Performance Analysis

A wireless sensor network which consists of sensor nodes is assumed, such as s_1, s_2, \dots, s_n , l_0 is the amount of overhead for a transmission; and l_t is the length of a tuple in a packet. The hop count from *node* to a base station is defined as $h(\text{node})$.

If one performs a virtual select operation at a base station, each node should send its tuple to a base station. Therefore, the total amount of transmission data for all sensor nodes is shown in (5)

$$(l_0 + l_t)h(s_i) + (l_0 + l_t)h(s_j) = (l_0 + l_t)(h(s_i) + h(s_j)) \tag{5}$$

where l_0 is the amount of overhead for a transmission and s_i and s_j are the nearest nodes to a location.

But if the query generates virtual tuples in the sensor nodes, two sensor nodes broadcast their tuple to nearby nodes and only a master node transmits a virtual tuple to the base station. Therefore, the total amount of transmission data to send a virtual tuple to a base station is shown in (6) and is less then or equal to (5) where s_i is the master node and $h(s_j) \geq 2$.

$$2(l_0 + l_t) + h(s_i)(l_0 + l_t) = (l_0 + l_t)(h(s_i) + 2) \tag{6}$$

Generally, the hop count from a sensor node to a base station is larger than 2 except at nodes nearby to the base station. Thus it is possible to reduce transmission data by generating virtual tuples in the sensor nodes.

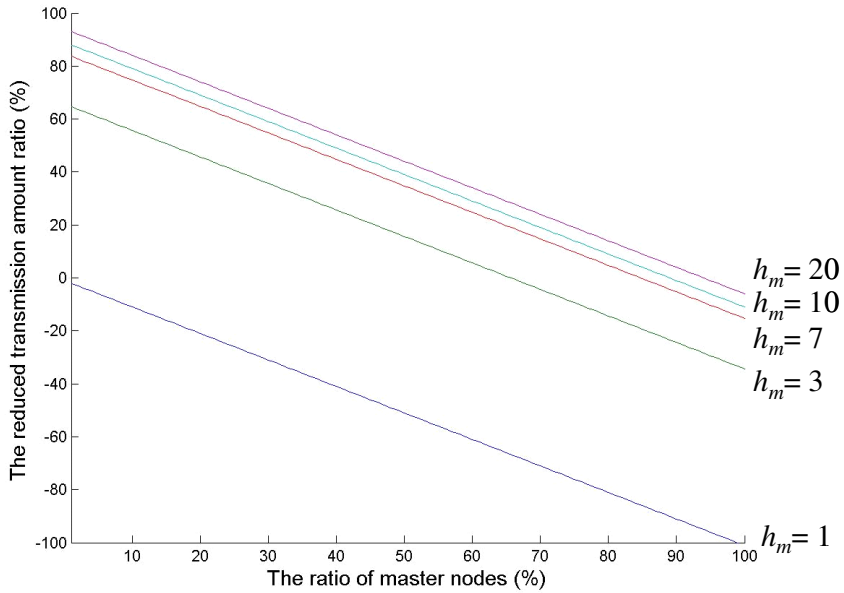


Fig. 3. The reduced transmission amount ratio according to the mean value of hops and the ratio of master nodes by the virtual select operation

If the mean value of hop counts h_m is used instead of $h(s_i)$, the equation for the ratio of the reduced amount of transmission data against the original amount of transmission data would be a function of h_m and $\frac{m}{n}$ like (7).

$$f\left(h_m, \frac{m}{n}\right) = 1 - \left(\frac{m}{n} + \frac{1}{h_m}\right) \quad (7)$$

Figure 3 describes graphs for (7) and shows how much transmission data are reduced by the virtual select operation generating virtual tuples in sensor nodes. In this figure, it can be shown that the ratio of the reduced transmission data is larger as the mean value of hops increases and the ratio of master nodes decreases.

6 Conclusion

Sensor nodes are deployed non-continuously in space and its locations are appeared as points. Therefore we can get sensing data at locations where sensor nodes are but cannot at elsewhere.

In this paper, we proposed the virtual select operation to generate virtual tuples. Adapting this operator to a wireless sensor network database, a user can simply pose a query that needs to estimate some attribute values in the database level. This also can

provide a standard interface to application programs and ensure more robust system. In addition, it enables to save energy which is one of the most important resource in wireless sensor networks by reducing the number of data transmission.

In underwater acoustic sensor networks, as acoustic waves need more transmission energy than radio waves and batteries are hard to be recharged or replaced, the proposed operation is more useful on underwater acoustic sensor networks.

A query optimization method for a virtual selection operator and a topology adaptive estimate method are important research topics and those will be explored in the future.

Acknowledgments. This research was supported by the MIC (Ministry of Information and Communication), Korea, under the 2007 ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

References

1. Govindan, R., Hellerstein, J., Hong, W., Madden, S., Franklin, M., Shenker, S.: The Sensor Network as a Database. Technical Report 02-771, Computer Science Department, University of Southern California (2002)
2. Heidemann, J., Silva, F., Intanagonwiwat, C., Govindan, R., Estrin, D., Ganesan, D.: Building efficient wireless sensor networks with low-level naming. In: Proceedings of the Symposium on Operating Systems Principles, pp. 146–159 (October 2001)
3. Karp, B., Kung, H.: Gredy Perimeter Stateless Routing. In: Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom 2000) (2000)
4. Bonnet, P., Gehrke, J., Seshadri, G.: Towards sensor database systems. In: Mobile Data Management, pp. 3–14 (2001)
5. Srivastava, M., Muntz, R., Potkonjak, M.: Smart Kindergarten: Sensor-Based Wireless Networks for Smart Developmental Problem-Solving Environments. In: Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom2001) (2001)
6. Hellerstein, J.M., Avnur, R., Chou, A., Hibder, C., Olston, C., Raman, V., Roth, T., Hass, P.J.: Interactive Database Analysis: The Control Project. *IEEE Computer* 32(8), 51–59 (1999)
7. Hellerstein, J.M., Haas, P.J., Wang, H.J.: Online Aggregation. In: Proc. ACM SIGMOID International Conference on Management of Data (1997)
8. Hellerstein, J.M., Avnur, R., Raman, V.: Informix under CONTROL: Online Query Processing. *Data Mining and Knowledge Discovery* 4(4) (October 2000)

GT² – Reduced Wastes Time Mechanism for Underwater Acoustic Sensor Network*

Soo-Young Shin and Soo-Hyun Park**

Graduate School of BIT, Kookmin University
{sy-shin, shpark21}@kookmin.ac.kr

Abstract. Recently, development of original technologies and connection technologies of UW-ASN for data transmission in underwater environment has been accelerated. Since propagation delay is inevitable at acoustic communication in underwater environment, the transmission time tends to be increased as network radius increases. Besides, there are difficulties of Multiple Access Control (MAC) service, which supports to avoid the collision and maintain reliable transmission condition. In this paper, a new scheduling method was proposed to eliminate the effect of interferences in a channel by taking both Gain-time and Guard-time into consideration.

Keywords: Underwater Acoustic Sensor Network (UW-ASN), MAC Scheduling, Gain-time and Guard-time (GT²).

1 Introduction

There are many different features in Underwater Acoustic Sensor network comparing with radio networks. One of those features is its narrow bandwidth caused by lower speed and very large propagation delay [1].

MAC should play a role of managing and controlling channels, which are shared by many nodes, to avoid collisions and to maintain reliable transmission condition. Under poor transmission environment, such as Underwater Acoustic Sensor network with narrow bandwidth and higher error rate, development of better MAC algorithm has been a critical issue. It is because the energy consumption of the communication system becomes larger and the cost of computing time and memory is also increased in case of re-transmission [2]. Besides, the condition of underwater acoustic transmission is much more inferior comparing to radio network in air [1]. In conclusion, MAC study plays a key role in its overall system performance.

Recently, many new scheduling and synchronization methods have been proposed to solve the problem of large propagation delay and transmission variance which is proportional to distance. Slotted floor acquisition multiple access (FAMA) was

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the 2007 ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

** Corresponding author.

proposed to reduce excessive waste of control packets [3]. MAC for Underwater Wireless Acoustic Network (UWAN) was proposed to solve synchronization problems and minimize the length of hand-shake procedure for non-synchronized ad-hoc UW-ASN [4][5]. Many research works, however, were the non-centralized contention-based multiple access control mechanism for ad hoc sensor networks. In underwater acoustic networks, three network topologies were proposed: centralized topology, single hop distributed topology and multi-hop topology[6][7][8]. This paper discusses Master Driven mechanism which is classified into MAC mechanism for centralized topology.

Common problem of underwater environment is a propagation delay regardless of what kinds of MAC are used. That is, the problem of propagation delay is not related to communication protocols. Generally, a Guard-time has been applied based on the maximum propagation delay of the network. However, GT^2 TDMA MAC scheduling technique proposed in this paper can be applicable to clustered networks. The proposed method is to increase the network efficiency by determining the moment of data transmission and data receipt adaptively taking the Gain-time and the Guard-time into consideration. In chapter 2, acoustic transmission model and the relationship between frequency bandwidth and the length of transmission data were investigated. In chapter 3, GT^2 transmission method was described. Finally, conclusion in chapter 4.

2 Underwater Environment and Acoustic Data Transmission

Analysis of marine environment is related to many parameters. For example, the speed of acoustic wave propagation is 1,500 meter per second in case of 20‰ of salinity and 22°C of water temperature while the speed decreases to 1,450 meter per second in case of 6°C of water temperature. As for water pressure, the acoustic wave speed increases as water pressure increases. In this paper, Mackenzie's Nine-terms algorithm [9], which is one of theories of sound speed, was selected to setup propagation model for definitions of marine environment parameters. Besides, transmission loss and noise model were selected for modeling errors caused by attenuation and various noises.

Table 1. Bandwidth and Distance

| Distance | Range [km] | Bandwidth [kHz] |
|------------|------------|-----------------|
| Very Long | 1000 | < 1 |
| Long | 10 ~ 100 | 2 ~ 5 |
| Medium | 1 ~ 10 | ≈ 10 |
| Short | 0.1 ~ 1 | 20 ~ 50 |
| Very Short | < 0.1 | > 100 |

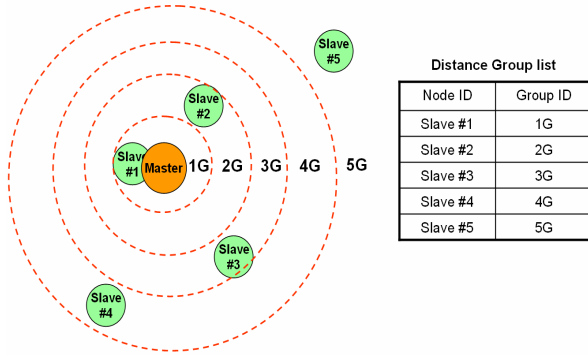


Fig. 1. Distance Group

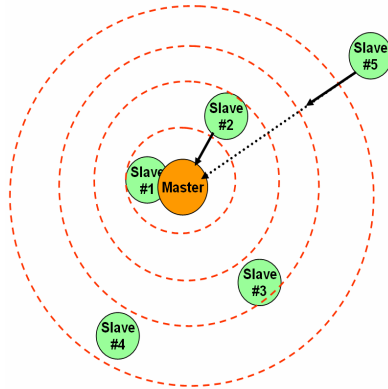


Fig. 2. An example of Distance Group

Acoustic wave can propagate farther as water depth increases and the wave speed determines the bandwidth. Table 1 shows relations between bandwidth and range (i.e. distance).

Acoustic wave speed in underwater condition is 1.5×10^3 m/s on the average which is faster by 4~5 times in air. Besides, the speed increases as water temperature, salinity and water pressure increase. In general, 1°C of temperature rise causes 3 m/s of wave speed increase. If water depth increases by 100 meters, the speed increase is 1.7 m/s. As for the effect of salinity, 1 ppt(precipitate) rise of salinity causes 1.3 m/s of speed increase. Generally accepted equation of acoustic wave speed calculation is as follows

$$c=1449 + 4.6T - 0.55T^2 + (1.39 - 0.012T)(S - 35) + 0.017Z$$

Where T is temperature in Celsius, S is salinity in p.s.u.(practical salinity unit), Z is water depth in decibar, c is speed in m/s.

3 GT² UW Transmission Model

3.1 Distance Group (DG)

DG is a transmission group classified by the distance between Slaves and Master. It is a concept introduced to differentiate propagation delay and guard band from DG. DG is known to all nodes in the network during network initialization procedure. Each node assigns adaptive time slot using node's order and group information. Figure 1 shows an example of DG. The concept of DG is based on the assumption that long distance transmission and the value of propagation delay affects Gain-time and Guard-time sufficiently. In addition, since deploy of nodes is relatively sparse, it is possible to applicable to most underwater acoustic sensor networks.

As shown in Figure 2, Slave #2 and #5 have difference DG of 2G and 5G respectively. That is, Slave #2 is closer to Master. In this case, data transmitted by two nodes do not collide even if these two nodes start transmission simultaneously since each other's distance to Master is different. Therefore, it is not efficient at all for Slave #5 to start transmission after Slave #2 finishes its transmission. In the proposed TDMA MAC scheduling, the concept of Gain-time, which is based on each nodes' distance to Master, is introduced. Based on the information of distance between Master and Slaves which can be obtained during network initialization procedure, each node is given its DG. The allocated DGs will be used for operation and allocation of time. Besides, since the Guard-time is also determined based on the value of DG. Figure 3 is a simplified diagram of GT² MAC technique showing the following two procedures. More detailed procedures are described in Table 2 and 3.

Table 2. Network Initialization procedure

| | |
|-----|--|
| (1) | <i>Master broadcasts Advertisement periodically</i> |
| (2) | <i>Slaves respond by sending join request message to Master</i> |
| (3) | <i>Master sets up the information of Distance Group information by using the information of Propagation Delay which were obtained during procedure (1) and (2)</i> |
| (4) | <i>Master broadcasts network configuration finished message with DGL to over all network.</i> |

Table 3. TDMA Scheduling procedure using GT²

| | |
|-----|---|
| (1) | <i>Master broadcasts Beacon frame, in which the information of reservation time slots is contained, for gathering the information of Slaves. At this moment, if there is any information received from slave(s) in the very previous round, Ack to the information is also transmitted. (Another research on this procedure is progressing as separate research item)</i> |
| (2) | <i>Slaves who received the Beacon transmit data during their assigned time.</i> |
| (3) | <i>After the corresponding round, a join procedure of new nodes, a periodic network reconfiguration procedure or setting-up new information requested by the network system can be conducted.</i> |

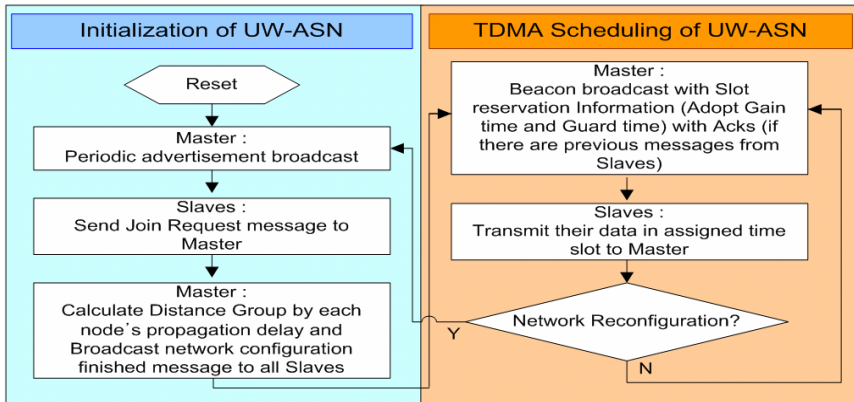


Fig. 3. Simplified Flowchart of GT² MAC

A distance-based concept Gain-time, which can be deduced during network initialization procedure, is introduced to give DG to each node. In the proposed GT² MAC Scheduling Scheme, therefore, it is intended that the concept of Gain-time according to distance interval is introduced and DG is given to all nodes on the basis of distance information between Master and Slaves which can be obtained during network initiation procedure. Besides, Guard-time is set by DG values. It is because as the distance increases the variation width with respect to transmission completion time also increases.

In proposed concept, all time units related to network operation is set to time slot. The size of unit time slot is already set in all underwater sensor network systems and determined on the basis of the distance and the frequency. It is a well known fact that the bandwidth is dependent on the center frequency so it is natural that the bandwidth is related to the length of time slot [9]. Time of underwater sensor network systems is calculated in slot unit and expressed as an integer value which can be an exact standard consequently.

3.2 Gain-Time and Guard-Time (GT²) Mechanism

In underwater sensor network systems, there is room for scheduling which is based on gains calculated from the delay time caused by media characteristics. In TDMA transmission procedure, DG of the previous node enables transmission delay time to be estimated. By referring to the delay time, the Gain-time can be estimated. The estimated Gain-time is calculated by unit of time slot and can be used during transmission. If the distance is not enough for obtaining Gain-time, 0 is set to Gain-time. In case of a network with large radius, which means the case of a long transmission distance, the gain calculated from Gain-time is also increases. Figure 4 shows an example of Gain-time and Guard-time.

Master puts the information of the assigned time slot and the transmission sequence of Slaves into Beacon and transmits the Beacon to the Slaves. Slave #2, #5 and #1 transmit data according to the pre-defined scheduling sequence and the pre-assigned time slot. In Figure 4, slave #2 and #5 obtained the Gain-time of 1 and 4

time slot, respectively. Slave #1 could not obtain any Gain-time. On Master's side, the probability of collision is avoided by assigning enough Guard-time when receiving data transmitted from each slave.

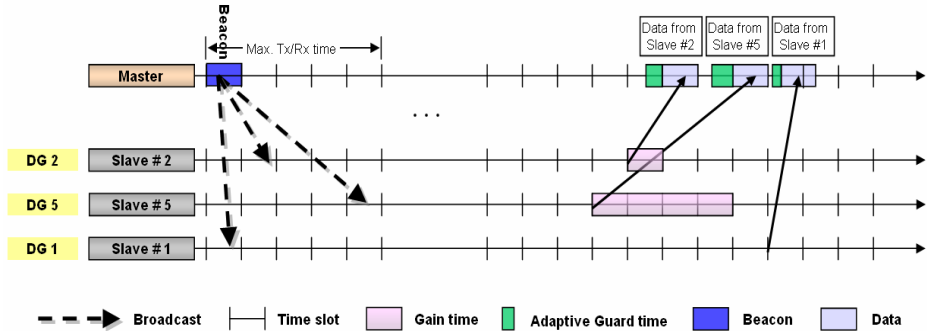


Fig. 4. An example of Gain-time and Guard-time

Guard-time is set taking the variation of transmission, which is possibly caused by irregular variations of underwater transmission environment, into consideration. It also can be set to be proportional to the distance between transmitting nodes. Since time variance is dependent on distance, it is required for Guard-time for listening to be adaptive against the distance between transmitting nodes. Figure 4 shows an adaptive Guard-time as well.

4 Conclusion

The proposed GT² TDMA MAC Scheduling method is applicable to Master/Slave structure cluster based networks. Taking that the majority of ocean and underwater sensor networks aim for exploration and monitoring into consideration, the proposed method is expected to contribute to development of more efficient MAC scheduling.

For future study, mathematical models will be developed for calculation of the proper size of time slot according to a network radius, the number of sensor nodes, frequency bandwidth and the packet length. Besides, using the model, exact Gain / Guard-time will be calculated and compared with the conventional methods. And the performance of the proposed method will be evaluated based on the comparison results.

References

- [1] Berkhovskikh, L., Lysanov, Y.: Fundamentals of Ocean Acoustics (1982)
- [2] Partan, J., Kurose, J., Levine, B.N.: A Survey of Practical issues in Underwater Networks. In: WUWNet 2006, pp. 17–24 (2006)
- [3] Molins, M., Stojanovic, M.: Slotted FAMA: A MAC Protocol for underwater Acoustic Networks. In: Proc. IEEE Oceans Conference (2006)

- [4] Rodoplu, V., Park, M.K.: An Energy-Efficient MAC Protocol for Underwater Wireless Acoustic Networks. In: OCEANS (2005)
- [5] Peleato, B., Stojanovic, M.: A MAC Protocol for Ad-hoc Underwater Acoustic Sensor Networks. In: WUWNet 2006 (September 2006)
- [6] Sozer, E.M., Stojanovic, M., Proakis, J.G.: Underwater acoustic networks. *IEEE journal of oceanic engineering* 25(1), 72–83 (2000)
- [7] Sozer, E.M., Stojanovic, M., Proakis, J.G.: Design and simulation of an underwater acoustic local area network. In: *Proceeding IEEE, Opanet 99, Washington (August 1999)*
- [8] Salva-Garau, F., Stojanovic, M.: Multi-cluster protocol for ad hoc underwater acoustic networks. In: *OCEANS 2003. Proceeding, vol. 1, pp. 91–98 (September 2003)*
- [9] Etter, P.C.: *Underwater Acoustic Modeling and Simulation*. Spon Press, London (2003)
- [10] Leroy, C.C., Parthiot, F.: Depth-pressure relationships in the oceans and seas. *J. Acoust. Soc. Amer.* 103, 1346–1352 (1998)

Comparative Evaluation of Probabilistic and Deterministic Tag Anti-collision Protocols for RFID Networks

Jihoon Choi and Wonjun Lee*

Division of Computer and Communication Engineering
College of Information and Communication
Korea University
wlee@korea.ac.kr

Abstract. Radio Frequency Identification (RFID) is an auto recognition system that consists of a number of tags and readers. There could be multiple tags a reader should identify. Since a medium is shared by multiple tags, a collision occurs at the reader's side when two or more tags get transmitted simultaneously. Therefore, anti-collision mechanism that collaborately arbitrates collisions is required. Tag anti-collision schemes can be classified into two approaches according to the way to determine the point of transmission time: probabilistic approach and deterministic approach. These two approaches show dissimilar performance according to situations because of difference of process property. In this paper, we analyze the most advanced ever-existing tag anti-collision schemes and standards, and evaluate the performance of them with newly proposed metrics in various network situations.

1 Introduction

Radio Frequency Identification (RFID) is an auto recognition system that consists of a number of tags and readers. A RFID reader identifies objects by reading the data contained in tags [1]. The RFID reader communicates with tags through radio frequency, which is performed in a different manner of the barcode system in which a reader identifies a barcode through the light. Due to these characteristics, the RFID has wider range of identification of tags such that tags can be identified even when line of sight (LOS) does not get obtained. For such reasons, the RFID system has been spotlighted as the technology which can replace barcode system.

Tags can be classified into two types based on the existence of self electric power: active tag and passive tag. The active tag can transmit data without the aid of a reader because it has its own battery. It also has a more powerful memory than a passive tag. On the other hand, it is possible for a passive tag to transmit only when a reader is involved since it does not support self electric

* Corresponding author.

power. A passive tag has constraints in functionality, but it has the distinct feature to the active tag: it is enough small to attach to an object easily. In this paper, we consider only passive tags.

There could be multiple tags a reader should identify. All the functionality tags should do is that they response with the data corresponding to the signal received from a reader. The communication between tags is impossible. Passive tags cannot make a decision of whether the channel is busy or not. A collision is occurred at the reader's side when two more tags get transmitted simultaneously. Therefore, the arbitrational mechanism is required. We call the protocol aiming to avoid collisions between a reader and tags anti-collision protocol. The anti-collision protocol should have the following characteristics.

- A reader should identify all the tags within its range.
- The anti-collision algorithm should have a mechanism which is capable of verifying that all the tags are identified.
- It should minimize the time elapsed for the identification of tags. It lies on same line as reducing collisions. As the time which is required to identify tags increases, it is more difficult to identify objects moving fast.

Tag anti-collision schemes can be classified into two approaches according to the way to determine the point of transmission time: probabilistic approach and deterministic approach. In this paper, we introduce various anti-collision schemes including AQS and ABS, which we have suggested in our previous work. We also evaluate their performance. This paper is organized as follows. We give a detailed description about probabilistic and deterministic anti-collision schemes in section 2. Section 3 introduces adaptive tag anti-collision algorithms, and is followed by performance metrics and evaluation in section 5 and section 6, respectively. Section 6 concludes the paper.

2 Backgrounds

Probabilistic tag anti-collision schemes are based on ALOHA. ALOHA is one of the basic medium access control mechanisms. In ALOHA, each tag generates a random number and waits for its transmission time according to the number chosen. If the data transmitted by a tag is not interfered by other data, the reader can identify the tag. A tag continues to do the same work after its transmission; generating a new random number and transmitting its own data after waiting for random amount of time. If during the interval two or more tags transmit, a collision occurs. In order to solve partial collision problems, transmission time is divided into discrete time intervals in the slotted ALOHA. All tags try to transmit their data after random back-off. If there are no partial collisions under the slotted ALOHA scheme, the slotted ALOHA doubles the channel utilization. A framed slotted ALOHA [2] [3] [4] [5] [6] groups some slots into a frame. A frame has several transmission slots. The starting point of frame and slot is synchronized by a message of a reader. Tags determine their transmission slot when they receive a starting message from a reader. Transmission slot is set by random number generator in tags.

The important factor which has influence on performance is the relation between the number of tags and random space, the maximum value of back-off timer. If the random space is larger than the number of tags in the reader's range, there can be many collision slots. On the other hand, if it is smaller than the number of tags, the frame may have too many idle slots. It is important to set suitable random space by predicting the number of tags.

According to the number of tag transmissions in a slot, slot can be divided into three types as follow:

- Readable slot: Exactly one tag transmits its data. The reader recognizes a tag successfully.
- Collided slot: More than two tags transmit their data. A tag collision occurs and the reader cannot recognize any tags.
- Idle slot: No tag transmits its data.

Under the frame slotted ALOHA schemes, the frame size means the size of random space. It is easy to change the frame size at each start of a frame. There exist many proposed schemes which improve the frame slotted ALOHA. The optimal frame size is the occasion when the number of tags and frame size are exactly the same. Many schemes that estimate the number of tags, using the number of readable slots, collision slots and idle slots, have been proposed. The symbol notions and their descriptions used throughout this paper are summarized in Table 1.

Table 1. Notations

| symbol | description |
|-----------------------|---|
| F | The frame size |
| N_{tag} | The estimated number of tags |
| S | The number of readable slots |
| C | The number of collided slots |
| I | The number of idle slots |
| $S_{EXP}(F, N_{tag})$ | The expected value of readable slots given frame size and the number of tags |
| $C_{EXP}(F, N_{tag})$ | The expected value of collided slots given frame size and the number of tags |
| $I_{EXP}(F, N_{tag})$ | The expected value of idle slots given frame size and the number of tags |

A readable slot which occurred in the previous frame is the one that contains only one tag. A collision slot has at least two tags. The lower bound of the number of tags can be estimated as Eq. (1).

$$V_{ogt1} : N_{tag} = S + 2C \tag{1}$$

In [4], the author proposed another way to estimate the number of tags. If we know the frame size and the number of tags, we can calculate the expected value

of readable slots, idle slots and collided slots. By using Chebyshevs inequality, we can make tag estimation function as Eq. (2).

$$Vogt2 : est_f = \min_{N_{tag}} \left| \begin{pmatrix} S_{EXP}(F, N_{tag}) \\ C_{EXP}(F, N_{tag}) \\ I_{EXP}(F, N_{tag}) \end{pmatrix} - \begin{pmatrix} S \\ C \\ I \end{pmatrix} \right| \quad (2)$$

The probability mass function of the number of reacting tag in a slot can be obtained by using binomial distribution. By using these probabilities, we are able to calculate the collision ratio [5], which is a fraction of the number of collision slots to the frame size. The number of tags can be obtained by Eq. (3).

$$DFSA : C_{ratio} = 1 - \left(1 - \frac{1}{F}\right)^{N_{tag}} \left(1 + \frac{N_{tag}}{F-1}\right) \quad (3)$$

Actually the number of tags in collision slot can be more than two. We can get the expected number of tags in collision slot approximately 2.39 tags [6]. We can estimate the number of tags by using Eq. (4).

$$Zhen : N_{tag} = S + 2.39C \quad (4)$$

Under deterministic tag anti-collision schemes, a tag determines the point of transmission upon receiving a message from a reader and making a process from the message. A reader divides tags into two groups. The reader divides the one of them into two groups once again. It is required that reader is able to distinguish each divided group. The process of dividing tags is continued until a group contains only one tag. The fact that the number of tags in that group is one means that a reader can identify the tag successfully. The dividing process of a group is continued until a reader identifies all the tags.

The reader transmits a query to tags under the query tree (QT) scheme [7]. The query contains the prefix of the tag identification (ID) codes. Every tag in range of reader compares the query of reader with its ID codes and transmits its ID codes to the reader in case the result of comparing is true. This scheme uses a query of reader, prefix of tag ID Codes, to divide tags into two groups. Tags in one group transmit their ID codes to the reader. Tags in the other group wait for next query of the reader. The content of query is identifier of each group. The reader repeats to divide tags into two groups until the number of tags in a group is one. When the number of tags in a group is one, the reader successes to identify one tag. This identification process can be considered constructing a searching tree based tag ID Codes. The reader increases the length of the query until the identification cycle is finished. Fig. 1 shows an example of the identification process using the query tree protocol.

The binary tree (BT) scheme [3] uses the pseudo random number generator to divide tags into two groups. The counter variable in each tag is used for identifying each group. At the beginning of identification operation, the reader sends the message which notifies the start of cycle to tags. All tags received this message generate a random number 0 or 1. Tags set their counter value by

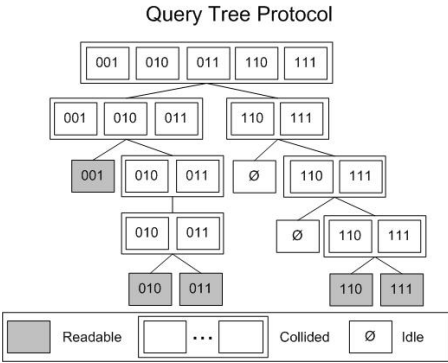


Fig. 1. An example of the identification process using the query tree protocol

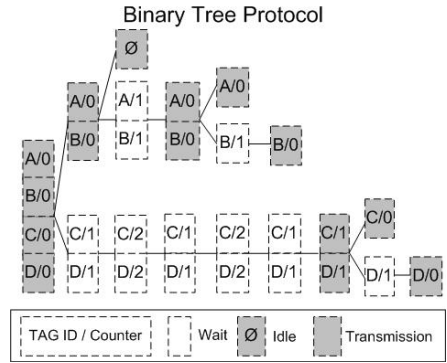


Fig. 2. An example of the identification process using the binary tree protocol

adding the random number. Tags are divided into two groups: one group has counter value of 0. The other group has counter value of 1.

The group with counter value of 0 tries to transmit and waits for the reply of the reader. If a collision occurs, tags which try to transmit in previous cycle are divided into two groups by using random number and tags which do not try to do increase the value of their counter by 1. If there is no collision, all tags decrease the value of their counter by 1. The tag identified successfully set the value of its counter to 0 and wait the start of frame message of the reader. Fig. 2 shows an example of the identification process using the binary tree protocol.

3 Adaptive Splitting Schemes

The main advantage of deterministic tag anti-collision scheme is that all tags in identification range of the reader can be identified. An identification cycle is a process that constructs a tree from root node to leaf nodes. When next identification cycle begins, information of tree in previous cycle is initialized. Following two schemes can improve the performance by using information of tree in previous cycle.

3.1 Adaptive Query Splitting

Adaptive Query splitting (AQS) [8] is our previous work and is the method that can reduce search space of current cycle by using the queries in leaf node of the tree which constructed in previous cycle. Searching from leaf node of the tree can diminish identification delay caused by query tree scheme which starts from root node of tree and can cover all possible search spaces.

The reader maintains not only the queue Q but also a candidate queue CQ. There are prefixes of tag ID codes in readable slots and idle slot from the previous

identification cycle in CQ. At the start of the identification process, the reader initializes Q with the CQ and empties out CQ.

Fig. 3(a) shows the operation of the adaptive query splitting protocol. If the population of tags is same as previous identification cycle, no collision occurs in current cycle under AQS scheme. If there exists an incoming tags whose ID matches a prefix of readable nodes in previous cycle, it decreases the number of collision nodes to use prefixes of readable nodes. If a new tag of which ID does not match a prefix of a readable node in previous cycle is quickly identified with prefixes of idle nodes in previous cycle by the reader.

To prevent the increase of CQ which carries information of leaf nodes uses the query deletion process. The query deletion process is the process that merges queries which are same except last one bit to one query.

3.2 Adaptive Binary Splitting

One of our previous work, Adaptive Binary Splitting (ABS) [9], is the method that has tags remember their identification order in previous cycle by adding one more counter in tags. The tag maintains progressed-slot counter (PSC) and allocated-slot counter (ASC). PSC means the number of timeslots passed in an identification cycle. At the start of an identification cycle, PSC is initialized with 0. In every readable slot, all tags increase their PSC by 1. ASC determine whether a tag can transmit its data or not. If a tag has ASC which is the same value as PSC, the tag can transmit.

The tag has three states as follows: 1. Wait state: If the tag has ASC greater than PSC, it waits for other commands of reader. 2. Active state: If the tag has ASC equal to PSC, it transmits its data to the reader. 3. Sleep state: If the tag has ASC less than PSC, the tag does not transmit any data. This tag waits for next identification cycle because it has already been identified in current identification cycle.

In the collided slot, the colliding tags, the tags of the active state, add a random number (0 or 1) to ASC. The active tags which select number 1 convert their state into wait state. The wait tags increase ASC, when collision occurs. When the reader send the message which means the idle slot to tags, the tags in the wait state decrease ASC.

Fig. 3(b) shows the operation of the adaptive binary splitting protocol. If the population of tag does not change, no collision and no idle occurs in current cycle under ABS scheme. The reader remembers the number of tags in previous cycle and informs tags of it at the start of identification cycle. If there are incoming tags, those tags randomly set their counter into smaller value than the number sent by the reader. Incoming tags can cause some collision with existing tags. When a collision occurs, those collided tags add a randomly selected binary number (0 or 1) to ASC. If there are leaving tags, idle slot can occur.

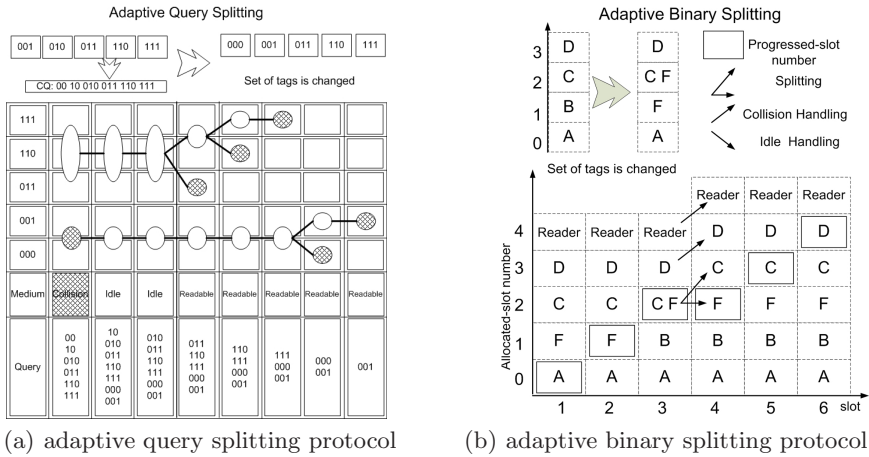


Fig. 3. The adaptive splitting protocols

4 Performance Metrics

RFID applications have various requirements. Mobility of tags is a key factor for branching properties of RFID applications. Mobility of tags varies according to what kinds of RFID applications are employed. In this section, we divide RFID applications into two cases. The first one is the case that has little mobility of tags. The second one is the case in which we have to consider mobility of tags for performing identification operation. In both cases, we present some points of reference for evaluating performance of RFID tag anti-collision protocols.

4.1 Total Identification Delay

For some applications, one can locate objects in front of a reader, which then are identified. Such a scenario falls under where a reader is deployed at an entrance or an exit at which the products are disposed of. In this case, a user should determine the starting point and wait until all tags are identified. In these kinds of applications, the time for identifying all tags in reader's range is a critical factor for evaluating performance of RFID tag anti-collision protocols.

4.2 The Number of Identified Tags

We can consider the situation where objects with a RFID tag move toward a reader through a conveyor belt. Under the situation of this kind, the relation between the velocity of conveyor belt and the number of identified tags can be considered as an important guideline to evaluate the performance of tag anti-collision protocols. The velocity of conveyor belt means the variation of tag

population. If a tag anti-collision protocol can identify many tags under the situation that tags go through the reader’s range fast, it means that the protocol can fast overcome the variation of tag set.

4.3 Re-identification Interval

In case a RFID reader has to recognize tags in reader’s range persistently, a reader continues to perform identification process. The shorter the length of identification cycle is, the frequenter tags are identified. If a anti-collision protocol can access same tag many times, that protocol can recognize fast whether the tag is in reader’s range or not. This can be described as re-identification interval and be an important factor for evaluating performance of RFID tag anti-collision protocols. The tag tracing can be performed precisely and quickly with decreasing the re-identification interval.

5 Performance Evaluation

In this section, we evaluate the performance of tag anti-collision protocols examined so far. We make following assumptions for reflecting only the effect on the operational principle of tag anti-collision protocols. Reliability in transmission between a reader and a tag is perfectly guaranteed. All the protocols consider make use of the same type of physical functionalities. All protocols have same time for transmitting their ID codes. The reader just targets tag identification and does not perform any additional operations.

The transmitted message format is set based on ISO 18000-6 specification. Fig. 4 describes data transmission between a reader and a tag. Since we would like to evaluate the performance of protocols based on transmission slots, we does not consider the computation delay between end point of data receiving and start point of data sending.

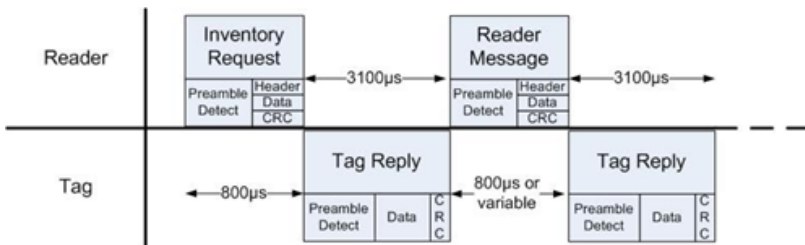


Fig. 4. Data transmission between a reader and a tag

5.1 Total Identification Delay

We perform simulation study to investigate how long a user should wait for at each protocol. As we assume that mobility of tags is not considered, a reader

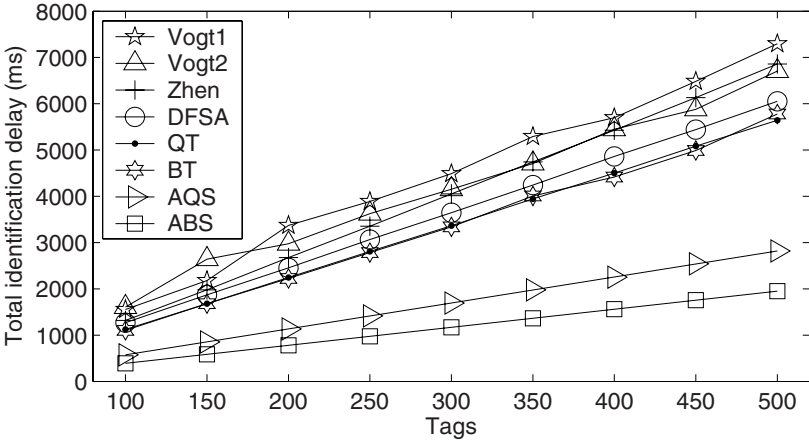


Fig. 5. Total identification delay

makes identification process without changes on tags sample during its identification.

Fig. 5 shows the relationship between the number of tags and the time taken to identify all tags by each protocol. Probabilistic tag anti-collision schemes are independent of each round, and keep three slots: the success, the readable, and the idle slot, all of which follows identical probabilistic distribution.

QT and BT, which belongs to the deterministic scheme, shows better performance than the probabilistic one. They are, however, little different in total identification delay. There is not much different in performance between probabilistic schemes until the samples are over 250. The reason why Vogts method becomes debased when samples over 300 is that it assumes the case where the maximum frame size is 256. In Zhen and DFSA, the predicted number of tags is employed as the frame size, so it outperforms Vogts when the number of tags increases. It is expected that both schemes can show the similar results provided that Vogts configure the frame size to the tags predicted. ABS and AQS experience the least delay out of the protocols. This is because they have already known information of the population of tags. That is, the simulation on them is performed after the identification is done once. Due to the inherent characteristics of ABS and AQS, under the same condition with BT and QT, we obtain the same results shown in them.

5.2 The Number of Identified Tags

This section presents performance of tag anticollision schemes in the applications with high mobility of tags. We consider the situation where objects with a RFID tag moves toward a reader through a conveyer belt. There can be tops 200 tags within its readers range. We measured performance varying the velocity of a conveyer belt.

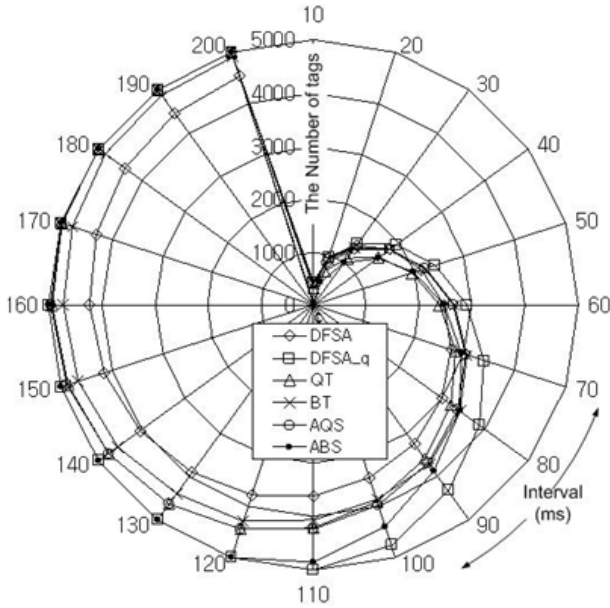


Fig. 6. The number of identified tags

Fig. 6 shows the identified number of objects at each anti-collision scheme when 5,000 objects get moved. The main purpose of this application aims to identify tags passing by a reader. In such an application, if tags are waken up in advance before identification process by a reader, we can have the advantage of adapting Quiet state of tags because the tag having been already identified does not need to perform that process again. We evaluate DFSA and DFSA_q (Quiet state) in Fig. 6.

As the speed of conveyer belt increases, the interval entering a readers range is reduced. In other words, the larger the interval increases, the slower the conveyer belt moves. DFSA using Quiet state succeed in identifying all tags of 5,000 even at the fastest condition. ABS is the second to them in adaptability of the speed of a conveyer belt.

The Probabilistic tag anti-collision schemes adapting Quiet state of tags outperforms since the number of tags is small in the initial part. The reader performs the identification operation with small number of tags and makes them sleep. In this case, the size of population is maintained at small size. On the other hand, because the tags which were already identified in pervious cycle rejoin the identification operation in current cycle in the deterministic tag anti-collision schemes, every cycle has more tags than the probabilistic tag anti-collision schemes adapting Quiet state.

Probabilistic tag anti-collision schemes without using the Quiet state of the tag cannot identify 5000 tags with 30ms interval due to rejoining of identified tags. AQS and query tree have similar performance and the performance of the

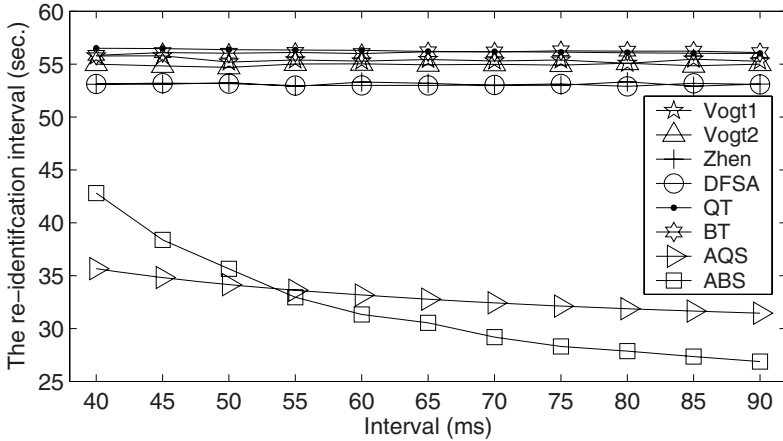


Fig. 7. Re-identification interval

binary tree is not good. However binary tree can identify all tags under the value of interval 0.026 per an incoming tag.

5.3 Re-identification Interval

We already define re-identification interval. As the application to make this metric be meaningful, we can consider the one where the state of the tags should be checked out in real-time. It is meaningless to use the Quiet state in such applications. It must be considered that the method to wake tag up in an appropriate timing. Because there has little investigated on such a method, we just compare the probabilistic tag anti-collision schemes without Quiet state with the deterministic ones.

In a conveyer belt, the interval and the moving speed of the tag can be regarded as the speed of the belt and the rate of changes of samples, respectively. Fig. 7 shows the re-identification interval per unit time. Given the interval is over 40 ms, since even probabilistic schemes without Quiet state achieves high identification ratio over 98 %, we depict the results from 40 ms in interval. ABS and AQS shows desirable results, while the other schemes are even. ABS and AQS achieves good performance than other schemes because they can take advantage of the identification information of the previous stage.

6 Conclusion

In this paper, we have introduced tag anti-collision schemes and evaluated the performance of them. According to the types of RFID applications, we considered two cases: motionless tags and moving tags. For applications employing motionless tags, a user can determine the start and end of the identification process. When such applications are considered, probabilistic and deterministic

tag anti-collision schemes show the similar ability in identifying tags. For applications requiring persistent observations on tags, AQS and ABS outperform any other schemes, especially under the situation that tag population varies at low speed. An important factor we should consider in evaluating performance of persistent observation is to identify whether a tag exists within its reader's range as quickly as possible. We also show that AQS and ABS are appropriate to meet this evaluating factor.

Acknowledgement

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MOST) (No. R01-2007-000-11203-0).

References

1. Finkenzeller, K.: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley & Sons, Chichester (2003)
2. EPCTM Radio-Frequency Identification Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz Version 1.0.8, EPCglobal (December 2004)
3. Information Technology Automatic Identification and Data Capture Techniques - Radio Frequency Identification for Item Management Air Interface - Part 6: Parameters for Air Interface Communications at 860-960 MHz, Final Draft International Standard ISO 18000-6.
4. Vogt, H.: Efficient Object Identification with Passive RFID Tags. In: Proc. of the International Conference on Pervasive Computing, pp. 98–113 (April 2002)
5. Cha, J., Kim, J.: Dynamic Framed Slotted ALOHA Algorithm Using Fast Tag Estimation Method for RFID System. In: Cha, J., Kim, J. (eds.) Proc. of the IEEE Consumer Communications and Networking Conference, Las Vegas, USA (January 2006)
6. Zhen, B., Kobayashi, M., Shimizu, M.: Framed ALOHA for multiple RFID objects identification. IEICE Transactions on Communications E88-B(3), 991–999 (2005)
7. Law, C., Lee, K., Siu, K.-Y.: Efficient memoryless protocol for tag identification. In: Proc. International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, pp. 75–84 (2000)
8. Myung, J., Lee, W.: An adaptive memoryless tag anti-collision protocol for RFID networks. In: Proc. IEEE INFOCOM (2005)
9. Myung, J., Lee, W.: Adaptive Splitting Protocols for RFID Tag Collision Arbitration. In: Proc. ACM MOBIHOC, pp. 202–213 (2006)

An Efficient Mutual Authentication Protocol on RFID Tags

Hui-Feng Huang

Department of Information Management
National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.
phoenix@ntit.edu.tw

Abstract. Recently, as low-cost radio frequency identification (RFID) becomes more pervasive in our daily lives, RFID systems may create new threats to security and privacy of individuals and organizations. It must have secure mutual authentication mechanisms to protect privacy information. However, the previous works on designing security protocols for RFID either do not conform to the EPCglobal Class 1 Generation 2 (GEN-2) standards or suffer from security flaws. In 2007, Chien and Chen proposed a mutual authentication protocol for RFID systems to improve the previous schemes. However, their scheme cannot efficiently retrieve the information of tags from its database for the authentication. To guarantee the quality of the growing popular communication services, it is urgent to construct efficient authentication for both parties of the tag and the back-end server such that the reader can quickly obtain the information of tag from its database. For light-weight calculation power of a tag and protecting the privacy of user (or product), this article proposes the RFID mutual authentication scheme based on GEN-2 standards. The proposed scheme can efficiently retrieve the information of tags from the database in the authentication process. Moreover, the proposed scheme can improve the previous schemes and provide anonymous property and forward secrecy.

Keywords: RFID system, security, authentication.

1 Introduction

Owing to low cost and conveniences in identifying an object without physical contact, radio frequency identification (RFID) systems will replace the optical barcode on objects with consumer identification, the radio frequency identification RFID systems can be used in lots of applications such as supply chain management, parking garage management, and inventory controls and so on [1]. Radio frequency identification (RFID) is an automatic identification system that can remotely store and retrieve data about objects by using small devices called RFID tags. RFID systems consist of radio frequency (RF) tags and RF readers. Tag readers can question tags about their contents by broadcasting an RF signal, without physical contact. RFID devices can be broadly classified in two categories: those with a power supply that actively transmit

to a reader are known as “active tags” and un-powered tags that are triggered by a reader are called “passive tags”. EPCglobal and ISO are two important organizations standardizing and promoting technology. Especially, EPCglobal has great potential to influence the standard for RFID technology at the global scale [1]. One of the most important standards proposed by EPCglobal is EPCglobal Class 1 Generation 2 RFID specification (which is called GEN-2 RFID for short in this paper) that defines the functionality and operation of a RFID tag.

The current RFID system allows any reader to access any tag. The exposed private information stored in the tag could be jeopardized. Then, the widespread deployment of RFID systems into consumer products identification may expose potential security threats and risks either to corporations or individuals. For example, a dishonest company may try to collect information of competing company about physical distribution. By utilizing responses from a tag, an adversary may try to get knowledge of products which an individual user carries or trace a user. Therefore, the security of the RFID is becoming more and more important. It must have mutual authentication mechanisms to identify the legal tag and legal tag reader. Some RFID implementation would expose tags identifications when readers inquire them. In addition, the most important security requirement for user privacy is untraceability [2,11]. With an untraceability property, an attacker cannot track tags by suing interactions with tags. That is the values emitted by a tag must not be discriminated from the other tags. With anonymity, tags will not expose their identifications to eavesdroppers without authentications. It can protect the tag from tracing over wide areas.

To cope with the security threats, there are several protocols had been proposed to enhance the security of RFID systems [2-10]. However, most of previous protocols required the support of either hash function or encryption function on the tag. These protocols for RFID do not conform to the EPCglobal Class 1 Generation 2 (GEN-2) standards. Because the adopted hash functions cannot be supported on the current resource limited GEN-2 RFID specifications. Only few proposed schemes can be implemented on GEN-2 RFID tags [2,5]. Unfortunately, these schemes still suffer from security weaknesses, and they cannot provide anonymity property or forward secrecy. In 2007, Chien and Chen [11] proposed a mutual authentication protocol for RFID systems to improve the above mentioned schemes [2-10]. Their scheme is not only providing anonymity property and forward secrecy but also conforming to the GEN-2 standards. However, in Chien and Chen’s protocol [11], when the server receives the authentication request from the reader, it must iteratively pick up an entry information from its database to find a match tag. If it can find a match, then the authentication of the tag succeeds; otherwise it cannot pass the authentication. Their authentication process is repeated for each entry until it finds a match. It is not efficient for the reader to obtain the information of tags. To guarantee the quality of the growing popular communication services, it is urgent to construct efficient authentication for both parties of the tag and the back-end server such that the reader can quickly retrieve the information of tag from the back-end database.

For light-weight calculation power and protecting the privacy of a user (or product), this paper proposes the RFID mutual authentication scheme based on GEN-2 standards. The proposed method can immediately pick up an entry from its database for the authentication between the tag and the back-end server. It need not iteratively repeated for each entry until it finds a match. Therefore, the proposed protocol is

more efficient than Chien and Chen's scheme for the authentication. Moreover, the proposed scheme could protect a user (product) from tracing and provide the forward secrecy.

The remainder of this paper is organized as follows. In the next section, we will propose the mutual authentication protocol based on the RFID system. The security analysis of the proposed scheme is presented in Sections 3. And some conclusions will be made in the last section.

2 The Proposed Scheme

This section will propose a new efficient mutual authentication protocol for RFID systems. The assumption, initial setup, and authentication process are described as follows:

2.1 Assumption and Initial Setup

The proposed scheme is based on the EPCglobal Class 1 Generation 2 standards (GEN-2), where PRNG (Pseudo Random Number Generator) and Cyclic Redundancy code (CRC) operator are supported on passive tags [1]. The reader R connects with a legal back-end sever that has database D . We assume an attacker (or illegal reader) can monitor and modify the communications between the reader and the tags, but the communication between the reader and the back-end server (database) is secure. Here, the function $h(\cdot)$ means the Pseudo Random Number Generator.

In the initial stage, tag t_i and the back-end sever share the identifier ID_i , a secret key k_i, n_i , and a function $h(\cdot)$. The number n_i is randomly selected by the back-end server for a tag t_i . The back-end database contains fields ID, N, K, K_{last} , and N_{last} which save the identity of tag t_i ; the current number of tag t_i , the current secret key k_i of tag t_i , the preceding secret key k_i^{last} , and the preceding number n_i^{last} , respectively. Here, the preceding k_i^{last} and n_i^{last} are the previous information which are replaced by the current values k_i and n_i , respectively. Based on GEN-2 standards, the tag and the reader R has the PRNG (Pseudo Random Number Generator $h(\cdot)$) to generate a random number for the authentication process.

Initially, the fields ID, N , and K are set up with the ID_i , the current number n_i , and the initial secret key k_i of each tag t_i , respectively; and all values of the field K_{last} and N_{last} are null in the back-end database. The roles of K_{last} and N_{last} are to prevent desynchronization.

Authentication Process

We depict the process of authentication between tag t_i and the back-end server as follows:

Step 1. Reader R generates and saves a new pseudorandom number s by utilizing PRNG, and sends s to tag t_i .

- Step 2. Tag t_i also generates a new pseudorandom number r_1 and computes $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$. Then, tag t_i sends r_1 , r_2 , and its current random number n_i to the reader R , where $\|$ is the concatenation of operations.
- Step 3. After receiving r_1 and r_2 , reader R delivers r_1 , r_2 , n_i , and s to the back-end server.
- Step 4. When the back-end server receives the authentication request from the reader R , according to the current number n_i from one of fields N and N_{last} , it picks up an entry information (ID_i, k_i, k_i^{last}) of tag t_i from its database. It then computes and checks whether any of the following two equations hold.

$$r_2 = h(r_1 \| k_i \| s) \oplus ID_i \text{ or } r_2 = h(r_1 \| k_i^{last} \| s) \oplus ID_i. \tag{1}$$

In equation (1), it is depending on which value of fields N and N_{last} matches the current number n_i . If field N matches n_i , it checks whether equation $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$ hold. Similarly, when the field N_{last} matches n_i , it checks whether equation $r_2 = h(r_1 \| k_i^{last} \| s) \oplus ID_i$ hold. If equation $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$ or $r_2 = h(r_1 \| k_i^{last} \| s) \oplus ID_i$ holds, then authentication of the tag t_i succeeds, and the server performs the next step; otherwise, it sends a “failure” message to the reader R to stop the process.

- Step 5. If the back-end server successfully authenticates tag t_i in step 4, it computes $r_3 = h(r_2 \| k_i \| s) \oplus ID_i$ or $r_3 = h(r_2 \| k_i^{last} \| s) \oplus ID_i$ depending on which value k_i or k_i^{last} satisfies in the verification equation (1) in step 4. It also updates the value of field N into $h(n_i \oplus k_i)$ and the value of field N_{last} into n_i ; and updates the value of field K into $h(k_i)$ and the value of field K_{last} into k_i if $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$ in equation (1); otherwise, it does not update the information of fields N, N_{last}, K , and K_{last} . Then, the server sends r_3 and the information of tag t_i to reader R .
- Step 6. The reader retrieves the information of tag t_i and forwards r_3 to tag t_i . Upon receiving r_3 , tag t_i computes $r'_3 = h(r_2 \| k_i \| s) \oplus ID_i$ by using its secret key k_i , and then checks if $r_3 = r'_3$. If it holds the current secret key k_i and random number n_i of tag t_i are replaced by $h(k_i)$ and $h(n_i \oplus k_i)$, respectively.

In the proposed scheme, it constructs a function chain of information as follows: The function chain starts from secret t , the second secret key x_2 is $h(t)$, and the other j -th element x_j is $h(x_{j-1})$ for each tag. Similarly, if a tag has the $(j-1)$ -th random number y_{j-1} and $(j-1)$ -th secret key x_{j-1} , then the j -th random number y_j is $h(y_{j-1} \oplus x_{j-1})$ for the tag. For security, the random numbers s and r_1 should be used only one time in the protocol. The above processes are briefly illustrated in Figure 1.

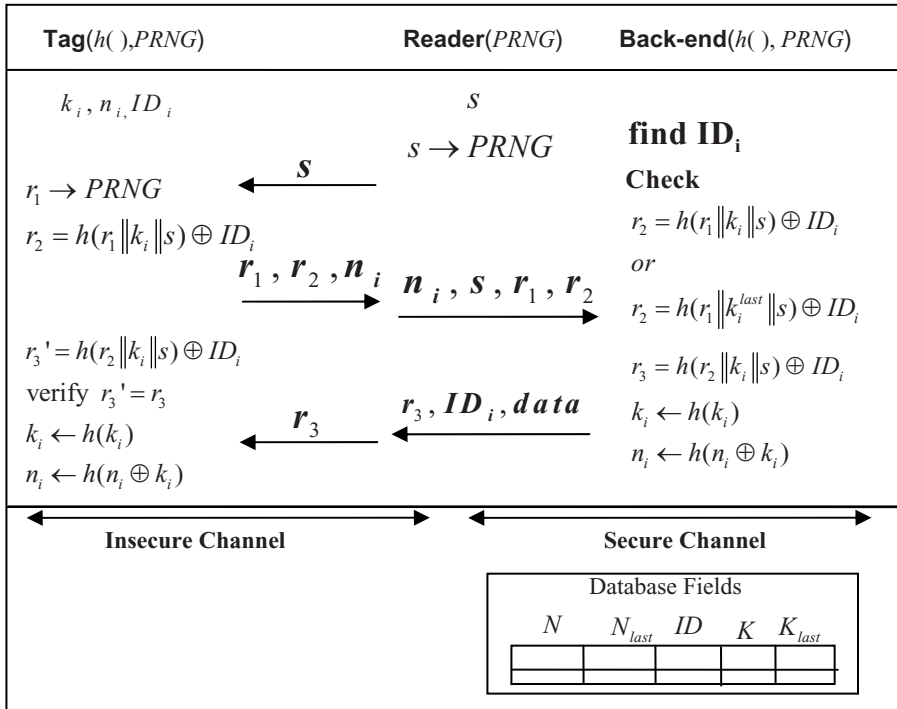


Fig. 1. The proposed Scheme

3 Security Analysis

In this section, we analyze the security of the proposed scheme. Due to the challenge of response technology and the freshness of random numbers s and r_1 per session, the proposed scheme achieves mutual authentication of the reader (server) and the tag, and can resist the replay attack. In the proposed method, the design of simultaneously maintaining the old key (or old number) and the new key (or new number) for each tag in the back-end database can resist the Denial of Services attack (DOS). That is, the back-end database has been replaced by the current (or new) key with $h(k_i)$ and the current number $h(n_i \oplus k_i)$; however, when reader R sends the “ r_3 ” command to tag t_i , it can suddenly be intercepted or modified by an attacker. Tag t_i will then hold the old key k_i and old number n_i . Thus, the shared information between the tag and the server (database) will be out of synchronization. In this situation, if the back-end database only keeps the new information $h(k_i)$ and $h(n_i \oplus k_i)$ for each tag, then the tag and the reader can no longer authenticate each other. Then, the back-end database can deny the services for the tag. The DOS attack succeeds. Therefore, in our scheme, the back-end database simultaneously maintains old information and new information which can then resist the DOS attack.

On the other hand, only randomized data (s, r_1, r_2, r_3, n_i) are transmitted on the wireless channel between the reader R and tag t_i ; and the information of tag t_i is only transmitted from the back-end sever to reader R through the secure channel. Therefore, the privacy and anonymity properties for tag t_i are ensured. With $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$ and $r_3 = h(r_2 \| k_i \| s) \oplus ID_i$, an attacker can obtain $h(r_2 \| k_i \| s) \oplus h(r_1 \| k_i \| s)$ by computing $r_2 \oplus r_3$. However, it is not helpful for him to retrieve the secret key k_i of tag t_i .

In the proposed scheme, the current number n_i is replaced by $h(n_i \oplus k_i)$ after each successful authentication. That is, the number n_i is only used one time. Therefore, without knowing the current secret key k_i of tag t_i , even if an attacker can obtain the data (s, r_1, r_2, r_3, n_i) in this session, it is very hard for him to trace the same tag t_i for the next communication by means of n_i . Moreover, because the secure key k_i and current number n_i are updated after each successful authentication and the key and current number are generated by applying the Pseudo Random Number Generator $h()$, the compromise of a tag would not lead to the tracing the previous communications for the same tag. It is very hard for an attacker to access the tags and trace the tags, hence forward secrecy is achieved. Therefore, the proposed scheme provides mutual authentication for a tag and the server in the RFID system and offers an anonymity property to protect tags from tracing. In summary, our scheme is not only resisting the replay attack and DOS attack but also providing forward secrecy, privacy property, and anonymity property.

With regard to the authentication process, in Chien and Chen's scheme [11], when the server receives the authentication request from the reader R , it iteratively picks up an entry information from its database to find a match tag. If it can find a match, then the authentication of the tag succeeds; otherwise it cannot pass the authentication. Their authentication process is repeated for each entry until it finds a match. It is not efficient for the authentication between the tag and the back-end server.

In the proposed scheme, the back-end database contains fields ID, N, K, K_{last} , and N_{last} which save the identity of tag t_i ; the current number of tag t_i , the current secret key k_i of tag t_i , the preceding secret key k_i^{last} , and the preceding number n_i^{last} , respectively. Here, the preceding k_i^{last} and n_i^{last} are the previous information which are replaced by the current values k_i and n_i , respectively. When the back-end server receives the authentication request from the reader R , according to the transmission number n_i of tag, from one of fields N and N_{last} , it can quickly provide an entry information (ID_i, k_i, k_i^{last}) of tag t_i from its database to achieve the authentication. It need not iteratively repeated for each entry until it finds a match. Therefore, the proposed protocol is more efficient than Chien and Chen's scheme [11] for the authentication.

4 Conclusions

For light-weight calculation power of a tag and protecting the privacy and confidential information of a user (product), we propose a new efficient RFID mutual authentication scheme based on GEN-2 standards. Through our authentication protocol, the reader can efficiently retrieve the information of tag from a database. Moreover, the proposed scheme provides forward secrecy and has the anonymity property that could protect a user (product) from tracing over wide areas. It is very convenient and efficient for many applications.

References

1. EPCglobal, <http://www.EPCglobalinc.org/>
2. Duc, D.N., Park, J., Lee, H., Kim, K.: Enhancing security of EPCglobal GEN-2 FRID tag against traceability and cloning. In: The 2006 Symposium on Cryptography and Information Security (2006)
3. Henrici, D., Muller, P.: Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In: IEEE International Workshop on Pervasive Computing and Communication Security-PerSec, pp. 149–153 (March 2004)
4. Lee, S.M., Hwang, Y.J., Lee, D.H., Lim, J.I.: Efficient authentication for low-cost RFID systems. In: International Conference on Computational Science and its Applications-ICCSA, pp. 619–627 (May 2005)
5. Karthikeyan, S., Nesterenko, M.: RFID security without extensive cryptography. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 63–67 (2005)
6. Molnar, D., Wagner, D.: Privacy and security in library RFID: issues, practices, and architectures. In: ACM Conference on Computer and Communications Security-ACM CCS, pp. 210–219 (October 2004)
7. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic approach to privacy-friendly tags. In: RFID Privacy Workshop (November 2003)
8. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing. LNCS, vol. 2802, pp. 201–212. Springer, Heidelberg (2004)
9. Rhee, K., Kwak, J., Kim, S., Won, D.: Challenge-response based RFID authentication protocol for distributed database environment. In: Hutter, D., Ullmann, M. (eds.) SPC 2005. LNCS, vol. 3450, pp. 70–84. Springer, Heidelberg (2005)
10. Yang, Y., Ren, K., Kim, K.: Security and privacy on authentication protocol for low-cost radio. In: The 2005 Symposium on Cryptography and Information Security (2005)
11. Chien, H.Y., Chen, C.H.: Mutul Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards. Computer Standards and Interfaces 29, 254–259 (2007)

HGLAP – Hierarchical Group-Index Based Lightweight Authentication Protocol for Distributed RFID System*

JeaCheol Ha¹, HwanKoo Kim¹, JeaHoon Park², SangJae Moon²,
Juanma Gonzalez Nieto³, and Colin Boyd³

¹ Dept. of Information Security, Hoseo Univ., 336-795, Korea
{jcha, hkkim}@hoseo.edu

² School of Electrical Eng. and Computer Science, Kyungpook National Univ.,
702-701, Korea

{jenoon65, sjmoon}@ee.knu.ac.kr
³ Information Security Institute, Queensland Univ. of Technology, GPO Box 2434,
Brisbane, QLD, 4001, Australia
{juamma, boyd}@isrc.qut.edu.au

Abstract. This paper presents a low-cost and secure authentication protocol to reduce the computational load on both the back-end database and the tags in a distributed RFID system. The proposed protocol is based on a hierarchical group-index to reduce the search time for a tag *ID* in the back-end database. Thus, when a tag is included in the k -th-level subgroup, the database system takes at most $(k + 1) \cdot \sqrt[k+1]{m}$ hash operations to find the tag to be authenticated, where m is the number of tags. Furthermore, the proposed protocol also guarantees most security requirements, including robustness against replay and spoofing attacks, synchronization, and indistinguishability.

Keywords: RFID system, authentication, distributed DB, group-index, indistinguishability, traceability.

1 Introduction

A Radio Frequency Identification (RFID) system consists of three parts: the RFID tags, RFID reader, and back-end databases. The insecure channel which is caused by an RF interface between the RFID reader and the tags leaves an RFID system vulnerable to various attacks, such as eavesdropping, spoofing, a replay attack, traceability, and message interrupt attack. One solution to protect tags from attack is authentication between the tag and the reader. However, due to the low computational power and storage space of the tags, a lightweight authentication protocol is needed that takes account of the tag's implementation limitations and back-end server's capacity.

* This research was supported by the MIC of Korea, under the ITRC support program supervised by the IITA (IITA-2007-C1090-0701-0026).

Several attempts to resolve the RFID authentication problem between the tag and the reader have already been made using physical technologies, including the ‘Kill command’ [13], ‘Active jamming’ [7], and ‘Blocker tag’ [7] approaches. Meanwhile, in 2004, Weis *et al.* [12,13] proposed a hash-lock protocol and randomized hash-lock protocol as cryptographic solutions. Yet, with the randomized hash-lock protocol, the identity of a tag, ID_k , is transmitted in the final step of authentication, making it vulnerable to a replay attack, spoofing attack, and location tracing. Dimitriou [1] also proposed a lightweight RFID authentication protocol that enforces user privacy and protects against cloning, however, there is no method for recovering synchronization when a state of desynchronization occurs. In 2006, Lee *et al.* [9] proposed an RFID mutual authentication scheme that introduces forward security (or forward traceability) to an RFID system, although finding the ID of a specific tag entails a heavy computational load on the back-end database. Plus, while the lightweight and resynchronous mutual authentication protocol proposed by Ha *et al.* [3] resolves the location tracing problem, forward security, a replay attack, and desynchronization attack, this protocol involves updating the tag’s ID in each session, which is unsuitable for a distributed database environment.

Rhee *et al.* [11] proposed a challenge-response authentication protocol based on a hash function that is robust against spoofing and replay attacks, plus location privacy is also guaranteed. Meanwhile, Juels and Weis [6] independently suggested improvements to the hash-lock protocol, making it similar to the scheme proposed by Rhee *et al.* [11]. Although both schemes are robust to several attacks, the computational load on the back-end database is heavy when authenticating a tag. Finally, a hash-based efficient authentication protocol for a ubiquitous computing environment was proposed by Choi *et al.* [2]. Nonetheless, even though this protocol only requires one hash operation in a tag, it still has several security weaknesses due to the use of counter information.

Existing authentication protocols can be divided into two categories: ID -constant systems, in which a tag’s ID is not updated, and ID -renewable systems, in which the ID can be changed to a new ID value in each session. In literature, the protocols presented by Dimitriou [1], Lee *et al.* [9], and Ha *et al.* [3] can all be categorized as ID -renewable systems, whereas the schemes developed by Rhee *et al.* [11] and Choi *et al.* [2] are ID -constant, making them suitable for a distributed database environment, where all the back-end databases use a unique ID .

Accordingly, this study presents a low-cost and secure mutual authentication protocol for a distributed database RFID system. The proposed protocol is based on a hierarchical group-index to reduce the search time for a tag ID in the back-end database. When a tag is included in the k -th-level subgroup, the database system only takes at most $(k + 1) \cdot \sqrt[k+1]{m}$ hash operations to find the tag to be authenticated, where m is the number of tags. In addition, the proposed protocol also guarantees most security requirements, including robustness against replay and spoofing attacks, synchronization, and indistinguishability.

The rest of this paper is structured as follows. Section 2 explains the security properties of an RFID system. Section 3 then analyzes several previous RFID systems as regards their security and efficiency. The proposed a new authentication protocol based on hierarchical group-index is presented in section 4, and its security and efficiency examined in section 5. Some final conclusions are then given in section 6.

2 Security Properties in RFID System

The RFID reader interrogates the tags using an RF signal, then transmits the collected data to the back-end database. As such, the channel between the reader and the tag is insecure. The back-end database then receives data from the reader and transmits certain services to a specific tag, such as product and price information etc. However, the channel between the reader and the database is considered as secure. Thus, an attacker can eavesdrop on the messages between the reader and the tags due to the insecure channel, then use intermediate information or useful responses to perform various enhanced attacks. It is also assumed that an adversary has the capability to transmit various malicious messages to the tag or reader, thereby performing a spoofing or replay attack. The communication messages between the tags and the reader can also be interrupted by an attacker to block the service. As a result, a message interrupt attack can create a state of desynchronization between the tag and the reader, due to an abnormal closing of a session, message blocking, or different *ID* updating between the tag and the database. Therefore, the various security threats resulting from an insecure channel can be categorized as follows:

- **Information leakage:** One RFID privacy problem is information leakage about a user's belongings. For example, a user may not want certain information known by others, such as ownership of expensive products, identification of personal medicine, and so on.
- **Spoofing and replay attack:** After an adversary sends a malicious query to a target tag, they collect the responses emitted by the tag. The attacker can then impersonate the reader using the messages collected from the tag. Conversely, an adversary can replay the reader's query to impersonate the target tag. An attacker can also impersonate a legal tag or reader by replaying certain useful messages.
- **Desynchronization attack:**
If the current *ID* for a tag is different to the one in the database, this is referred to as a state of desynchronization. Thus, if an adversary blocks certain messages transmitted between a tag and the reader, a dysynchronization state can be created in an *ID*-renewable RFID system. If the *ID* of a tag is desynchronized, the tag can be easily traced, as one of the values emitted from the tag will be constant, thereby compromising the location privacy.
- **Location tracing attack:** Here, an adversary can obtain some useful information on a tag's location. This attack is essentially applied to a rigid RFID

system in which certain communication messages between the tag and the database are identical to those used in the previous session.

Consequently, various security requirements are needed for secure RFID authentication, as identified in previous literature [5,9,12]. The information leakage problem can be easily solved by using an anonymous ID for each product, then checking whether it is in the database or not. Meanwhile, to prevent a spoofing or replay attack, the protocol should satisfy an authentication requirement, whereas a mutual authentication protocol is needed when an adversary has the ability to impersonate a tag or the reader. If a tag's response does not depend on any reader input, as shown in [13], the tag's messages can be used in a replay attack.

One of the aims of a desynchronization attack is to spoil a tag by disturbing the ID search in the database. The other powerful threat is location tracing by successive desynchronization. If an adversary continuously blocks certain legal messages in a wireless channel, they can find a historical trace. Then, even though the adversary does not know the tag's ID , they can still trace the target tag if certain specific message patterns for the tag are found, *e.g.*, transmitted data that is increased by one for every session using a counter. Thus, for perfect location privacy, an RFID system should satisfy both indistinguishability and forward security, where the former means that the values emitted by one tag should not be distinguishable from the values emitted by other tags, while the latter means even if an attacker obtains the secret data stored in a tag, the location of the tag can not be traced back using previous known messages, *i.e.*, disclosed data or communication information.

3 Analysis of Related Works

3.1 Lightweight Challenge-Response Protocol: LCRP

Dimitriou [1] proposed a lightweight challenge-response RFID authentication protocol (LCRP) that guarantees user privacy and protects against cloning. However, since an attacker can block the final message transmitted from the reader to the tag, this means the tag and back-end database update using different keys, where the back-end database renews the secret key, while the tag keeps the old value, resulting in a state of desynchronization and making the target tag useless. In addition, an attacker can trace a tag by successively sending a query from the reader in a desynchronization state. As the tag will respond with the same message $H(ID_i)$, since the ID_i is fixed in a desynchronized session, the tag cannot satisfy indistinguishability.

3.2 Synchronized Secret Information Based Protocol: SSIP

Lee *et al.* [9] proposed an RFID mutual authentication scheme that utilizes a hash function and synchronized secret information. This scheme offers the most enhanced security properties with respect to user privacy, including resistance against tag cloning by allowing an additional hash operation. In particular,

they introduce forward security (or forward traceability) to an RFID system, and prove that their scheme is perfectly indistinguishable and almost forward secure. However, the back-end database is required to perform about m hash operations to find the specific ID related to a tag.

3.3 Lightweight and Resynchronous Mutual Authentication Protocol: LRMAP

Ha *et al.* [3] proposed an efficient RFID protocol to reduce the computational load on both the back-end database and the tags, while also guaranteeing most security requirements. Plus, in the case of desynchronization resulting from communication failure or a malicious attack, synchronization can be recovered between the database and a tag. However, the scheme is only suitable for a single database system, as the ID used in this protocol is renewable, as with the above two protocols.

3.4 Challenge-Response Based Mutual Authentication Protocol: CRMAP

More recently, Rhee *et al.* [11] independently proposed a challenge-response authentication protocol based on a hash function that is almost the same as the improved randomized hash-lock scheme. This scheme is robust against a spoofing attack, replay attack, and location tracing attack. Nonetheless, the scheme is still vulnerable to forward security, as the ID is not changed with every session. Plus, this protocol is inefficient in terms of the computational load, as the back-end database is required to perform on average $m/2$ hash operations for an ID search, where m is the number of ID s.

3.5 One-Way Hash Based Low-Cost Authentication Protocol: OHLAP

A computationally efficient RFID authentication protocol, OHLCAP, based on a hash function for a ubiquitous computing environment was proposed by Choi *et al.* [2]. Although this protocol only requires one hash operation in a tag, it still has certain security weaknesses, including the possibility of location tracing based on the leakage of counter information, an impersonation attack by maliciously updating a random number, and traceability based on a physically attacked tag [84].

4 Hierarchical Group-Index Based Lightweight Authentication Protocol: HGLAP

4.1 Notations

The following notations are used for the entities and computational operations to simplify the description.

- T : RFID tag or transponder
- R : RFID reader or transceiver
- DB : back-end database or back-end server
- $H(\cdot)$: one-way hash function, $H : \{0, 1\}^* \rightarrow \{0, 1\}^l$
- ID_i : i -th identity of tag, l bits
- GI^1 : first group-index of tag, l bits
- GI^k : last k -th depth group-index of tag, $GI^1 \supset GI^2 \supset \dots \supset GI^k$
- $r_R(r_T)$: random number generated by reader(tag), l bits
- $\{A^k\}$: set of messages from A^1 to A^k , that is, $(A^1||A^2||\dots||A^k)$
- Query* : request generated by reader
- $B_R(B_L)$: right(left) half of message B
- \oplus : exclusive-or(xor) operation
- $||$: concatenation of two inputs

4.2 System Model and Assumptions

One of the disadvantages in an ID -constant RFID system is the computational load on the back-end database when searching for a tag to be authenticated. As such, the proposed protocol focuses on two design concepts: 1) an authentication protocol suitable for a distributed database system that is achieved using a constant ID and 2) a low-cost protocol with a low computational load for both the database and the tag.

The DB divides the tag identities into several groups. If the total number of tags is $m(= g_1 \cdot m_1)$, the DB divides the tags into g_1 groups, with m_1 tags in the 1st-level group. Thereafter, if the number of tags in the 1st-level group is $m_1(= g_2 \cdot m_2)$, the DB further divides the tags into g_2 groups, with m_2 tags in the 2nd-level group. Using this way of grouping, up to k th-level groups can be created. A tag is then included in the 1st-level group to the k th-level group, that is, $T \in GI^k \subset GI^{k-1} \subset \dots \subset GI^1$ and $m = g_1 \cdot g_2 \cdot \dots \cdot m_k$. For example, Fig. 1 shows the case where the group level $k = 2$, the number of tags $m = 30$, the number of 1st groups $g_1 = 5$, the number of 2nd groups $g_2 = 2$, and the number of tags in a 2nd group $m_2 = 3$. The data field of the DB is composed of the

| 1st GI | 2nd GI | ID |
|----------|--------------|-----------|
| GI_1^1 | $GI_{1,1}^2$ | ID_1 |
| | | ID_2 |
| | | ID_3 |
| | $GI_{1,2}^2$ | ID_4 |
| | | ID_5 |
| | | ID_6 |
| \dots | \dots | ID_7 |
| GI_5^1 | $GI_{5,2}^2$ | \dots |
| | | ID_{30} |

Fig. 1. Hierarchical Group-index in DB ($k = 2$, $m = 30$, $g_1 = 5$, $g_2 = 2$, $m_2 = 3$)

group-index $\{GI^k\}$ and the ID s for each tag. Thus, a tag has a data field, such as $\{GI^k\}$, and an ID .

Normally, it can be assumed that a distributed system is used for a large system, where the DB will include information on a large number of tags. Thus, the time taken to search for an ID in the DB is a very important factor related to the system performance. Therefore, the hierarchical group-index model is useful for a fast ID search in a DB , as it provides flexibility between the number of group levels and the computational costs, i.e., the more group levels GI^k , the lower the computational speed for an ID search.

4.3 Protocol Description

Thus, a secure authentication protocol is presented based on a k -level group-index. In the proposed protocol, a tag T is included in the first-level group GI^1 , in the second group GI^2 , which is a subgroup of the first group, and in the final group GI^k , i.e., $T \in GI^k \subset \dots \subset GI^2 \subset GI^1$, where the parameter k means the subgroup level. Simply, if $k = 1$, a tag is only an element of the first-level group. Therefore, the group level is used to find a specific tag in the back-end database. Fig. 2 shows the process of the proposed HGLAP, and the following gives a detailed description of each step:

1. The reader sends a *Query* and r_R to a tag.
2. The tag generates a random number r_T and computes $A^j = H(GI^j || r_R || r_T)$ for all $j = 1, 2, \dots, k$ for searching the ID and $B = H(ID || GI^k || r_R || r_T)$ for authenticating the tag in the DB . Then, the tag sends B_R , r_T , and $\{A^j\}$ to the reader.
3. The reader forwards B_R , r_T , and $\{A^j\}$ with r_R to the back-end database.
4. The back-end database finds GI^k by checking $A^j = H(GI^j || r_R || r_T)$ for all $j = 1, 2, \dots, k$, then finds the real ID in GI^k by checking B_R . The back-end database authenticates the tag by checking that the computed B_R equals the received one. If it is true then the back-end database sends the B_L to the reader as a response.
5. The reader forwards the B_L to the tag.
6. The tag authenticates the reader by checking whether the received B_L equals the one computed in Step 2.

5 Security and Efficiency Analysis

5.1 Security

The security of the proposed HGLAP was evaluated against the threats described in Section 2.

- **Information leakage:** To obtain secret information from a tag, an adversary must be able to guess the ID . However, an adversary cannot compute the ID from $B = H(ID || GI^k || r_R || r_T)$ or $A^j = H(GI^j || r_R || r_T)$ due to the security property of a one-way hash function.

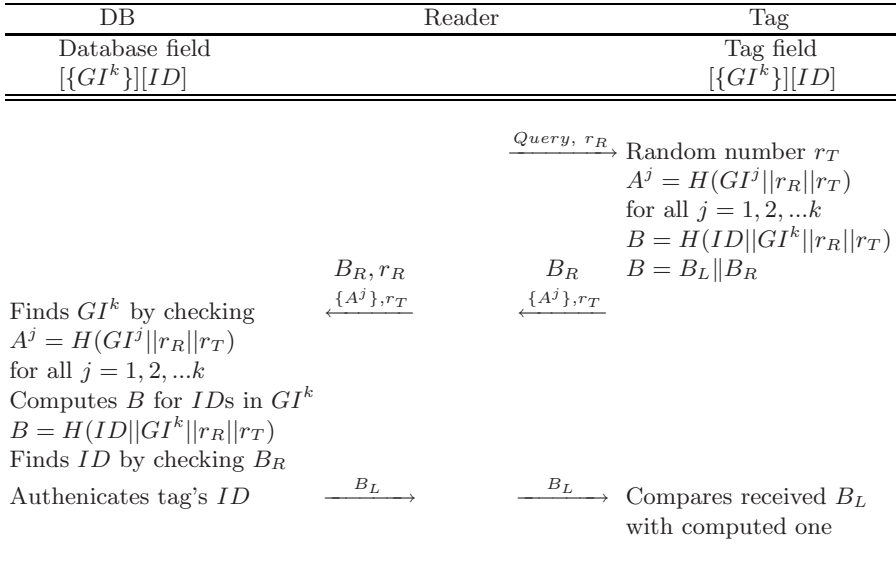


Fig. 2. Hierarchical Group-index based Authentication Protocol

- **Spoofing and replay attack:** Here, an adversary collects a tag’s responses, then tries a spoofing attack by impersonating a legitimate tag. However, an adversary cannot compute the hashed messages A^j and $L(B)$ without knowing the ID . Meanwhile, it is also impossible to impersonate a reader, as an adversary must send the correct $R(B)$, which can not be computed without knowing the ID value. Furthermore, even though an attacker can send a constant random number r_R to a tag, a replay attack can not compromise the proposed protocol, as A^j or B is refreshed by including a random number r_T in each session.
- **Desynchronization attack:** In a desynchronization attack, if the message loss occurs due to an adversary, the proposed protocol allows the tag and reader to detect this. First, it is assumed that an adversary blocks the response messages transmitted from a tag, *i.e.*, step 2 in Fig. 2 or a message from the reader, *i.e.*, step 5. However, since desynchronization attacks generally occur in an ID -renewable system, due to desynchronization between the back-end database and a tag, the proposed scheme is not affected by blocking, as it has a constant ID . Therefore, the back-end database and tag always maintain a synchronized state.
- **Location tracing attack:** The proposed protocol guarantees location privacy by randomizing the transmitted messages in each session. After the authentication is completely finished in the previous session, the tag sends A^j and $L(B)$ in response to a query in the current session. Thus, indistinguishability is satisfied as the values in the previous session have already been refreshed using two random numbers, r_R and r_T . As regards forward

Table 1. Comparison of security and efficiency

| Protocol | LCRP [1] | SSIP [9] | LRMAP [3] | CRMAP [11] | OHLAP [2] | Proposed |
|----------------------|--------------|-----------------|--------------|-----------------|--------------|---------------------------------------|
| Information leakage | O | O | O | O | O | O |
| Spoofing attack | O | × | O | O | × | O |
| Replay attack | O | O | O | O | O | O |
| Indistinguishability | × | O | O | O | × | O |
| Forward security * | △ | △ | △ | × | × | × |
| Resynchronization | × | O | O | O | O | O |
| Hash # of DB | 4 | $\frac{m}{2}+3$ | 3** | $\frac{m}{2}+2$ | 1 | $\frac{(k+1) \cdot \sqrt[k+1]{m}}{2}$ |
| Hash # of tag | 4 | 3 | 3 | 2 | 1 | $k+1$ |
| DB's storage | $2l \cdot m$ | $3l \cdot m$ | $3l \cdot m$ | $l \cdot m$ | $4l \cdot m$ | $(k+1)l \cdot m$ |
| Tag's storage | l | l | $l+1$ | l | $5l$ | $(k+1)l$ |
| Comm. load | $5l$ | $4l$ | $4l$ | $4l$ | $4l$ | $(k+3)l$ |
| Database | single | single | single | distributed | distributed | distributed |

O: secure or supported △: partially secure ×: insecure or not supported.
 *: Systems marked with △ are *ID*-renewable, those marked with × are *ID*-constant.
 **: $m+3$ required on average to recover synchronization.

security, if it is assumed that an attacker obtains a tag’s correct *ID* at some time, an adversary can then collect all the communication messages up to the time of obtaining the target secret *ID*, allowing the adversary to trace the past history of *B*, as the tag *ID* is not changed. Therefore, the proposed protocol cannot guarantee forward security, which is an inherent property of *ID*-constant systems.

A security comparison with previous authentication protocols is presented in Table 1. Therefore, with the exception of forward security, the proposed HGLAP was shown to be secure against most attacks, including a replay attack, spoofing attack, desynchronization attack, and location tracing attack.

5.2 Efficiency

When evaluating the computational load and storage costs for the *DB* and tag, as shown in Table 1, HGLAP exhibited a remarkable improvement in the computational cost for the *DB*. Although the challenge-response-based protocol [11] satisfies most security items, except forward security, its critical disadvantage is that the *DB* is required to perform $m/2+2$ hash operations to authenticate a tag. Thus, if it is assumed that a distributed RFID system is scalable and appropriate for a large system with lots of tags, the processing time required for the *DB* is a critical problem. As such, the computational cost in the *DB* has a trade-off relationship with the group-index level, where the higher the group-index level of a tag, the greater the storage space and computational load.

Yet, the computational cost in the *DB* can be reduced to at most $(k+1) \cdot \sqrt[k+1]{m}$ hash operations to find a tag, $\frac{(k+1) \cdot \sqrt[k+1]{m}}{2}$ on average. Thus, the

proposed protocol is very flexible as regards the computational cost in the *DB* and tag. When the group-index level k is just one, *DB* in the proposed protocol requires \sqrt{m} hash operations. On the other hand, *DB* in OHLAP only requires just one hash operation. However OHLAP has serious security flaws, including vulnerability to spoofing attacks and indistinguishability.

With the proposed protocol, the storage size of the *DB* is $(k + 1)l \cdot m$, where k is the length of an *ID* or hashed value and m is the number of *IDs*. Plus, a tag requires $(k + 1)l$ bits of memory to store an *ID* and the *GI* value. The total length of the messages transmitted from a tag to the reader is $(k + 1.5)l$, while that from the reader to a tag is $1.5l$, except for a *Query*. Therefore, the proposed HGLAP is suitable for a distributed RFID system with limited memory space and computational power.

6 Conclusion

A lightweight and flexible authentication protocol, HGLAP, was proposed to reduce the search time in the *DB*. The proposed protocol is suitable for a large-scale distributed RFID system, as it uses a constant *ID* for a tag. Furthermore, the proposed scheme is based on a hierarchical group-index for a fast tag-search operation in the *DB*. As regards the computational cost, HGLAP is designed to reduce the computational load on both the back-end database and the tags. When analyzed for security against existing attacks, the proposed protocol was shown to guarantee untraceability, authentication, and robustness against replay and spoofing attacks.

References

1. Dimitriou, T.: A lightweight RFID protocol to protect against traceability and cloning attacks. In: Security and Privacy for Emerging Areas in Communications Networks-2005. SecureComm 2005, pp. 59–66 (September 2005)
2. Choi, E., Lee, S., Lee, D.: Efficient RFID Authentication Protocol for Ubiquitous Computing Environment. In: Enokido, T., Yan, L., Xiao, B., Kim, D., Dai, Y., Yang, L.T. (eds.) Embedded and Ubiquitous Computing – EUC 2005 Workshops. LNCS, vol. 3823, pp. 945–954. Springer, Heidelberg (2005)
3. Ha, J.C., Ha, J.H., Moon, S.J., Boyd, C.: LRMMap: Lightweight and Resynchronous Mutual Authentication Protocol for RFID System. In: ICUCT 2006. proceeding of International Conference of Ubiquitous Convergence Technology (2006)
4. Ha, J.C., Moon, S.J., Nieto, J.G., Boyd, C.: Security Analysis and Enhancement of One-Way Hash based Low-Cost Authentication Protocol (OHLCAP). In: SSDU-2007 Workshop, Nanjing China (May 2007)
5. Juels, A.: RFID Security and Privacy: A Research Survey. RSA Laboratories (2005)
6. Juels, A., Weis, S.A.: Defining strong privacy for RFID, Cryptology ePrint Archive, Report 2006/137, Referenced 2006 (2006), at <http://eprint.iacr.org>
7. Juels, A., Rivest, R.L., Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for consumer Privacy. In: Security 2003. Proceeding of 10th ACM Conference on Computer and Communications, pp. 103–111 (2003)

8. Kwon, D., Han, D., Lee, J., Yeom, Y.: Vulnerability of an RFID Authentication Protocol Proposed in at SecUbiq2005. In: Zhou, X., Sokolsky, O., Yan, L., Jung, E.-S., Shao, Z., Mu, Y., Lee, D.C., Kim, D., Jeong, Y.-S., Xu, C.-Z. (eds.) EUC workshop 2006. LNCS, vol. 4097, pp. 262–270. Springer, Heidelberg (2006)
9. Lee, S., Asano, T., Kim, K.: RFID Mutual Authentication Scheme based on Synchronized Secret Information. In: proceedings of the SCIS 2006 (2006)
10. Lee, Y.K., Verbauwhed, I.: Secure and Low-cost RFID Authentication Protocols. In: 2nd IEEE International Workshop on Adaptive Wireless Networks (AWiN) (November 2005)
11. Rhee, K., Kwak, J., Kim, S., Won, D.: Challenge-Response Based on RFID Authentication Protocol for Distributed Database Environment. In: Hutter, D., Ullmann, M. (eds.) SPC 2005. LNCS, vol. 3450, Springer, Heidelberg (2005)
12. Sarma, S.E., Weis, S.A., Engels, D.W.: Radio-Frequency Identification: Security Risks and Challenges. RSA Laboratories 6(1) (Spring 2003)
13. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing 2003. LNCS, vol. 2802, Springer, Heidelberg (2004)

Target Classification in Sparse Sampling Acoustic Sensor Networks Using IDDC Algorithm*

Youngsoo Kim, Daeyoung Kim, Taehong Kim, Jongwoo Sung, and Seongeun Yoo

Real-time and Embedded Systems Laboratory,
Information and Communications University (ICU),
119 Munjiro, Yuseong-Gu, Daejeon, Korea, Postal Code: 305-714,
Phone: +82-42-866-6811; Fax: +82-42-866-6810
{pineland, kimd, damiano, jwsung, seyoo}@icu.ac.kr

Abstract. The analysis of time series using data mining techniques can be effective when all targets have their own inherent patterns in a sparse sampling acoustic sensor network where no valid feature of frequency can be extracted. However, both problems of local time shifting and spatial variations should be solved to deploy the time series analysis. This paper presents time-warped similarity measure algorithms in order to solve the two problems through time series, and we propose the IDDC (Improved Derivative DTW-Cosine) algorithm to deliver the optimal result and prove the performance with some experiments. The experimental results show that the object classification accuracy rate of the proposed algorithm outperforms the other time-warped similarity measure algorithms by at least 10.23%. Since this proposed algorithm produces such a satisfactory result with sparse sampling data, it allows us to classify objects with relatively low overhead.

1 Introduction

The target classification using sparsely sampled data is one of the key issues of a Wireless Sensor Network (WSN) application since it consists of a large number of low-power and inexpensive sensor nodes. When distributed sensor nodes sense and transfer data to a base station (BS) through WSN, the network cost might increase dramatically as the hop count increases. Especially in the case of acoustic data, while it is one of the most frequently used and informative sensors in a target classification system, it is so complicated and variable that it needs more numerous and dense data to obtain sufficient information. The bigger the WSN is, the less data should be basically transferred to increase the life span. It is because the mechanism of sensing frequently and transferring all of the data causes the nodes to be exhausted very fast.

Most of the existing research [1][2][3] for classification in acoustic WSNs have extracted features using the FFT and classified targets with some classification

* 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 Advancement)(IITA-2006-C1090-0603-0015) and the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government(MOST) (No. R0A-2007-000-10038-0).

algorithms such as k-nearest neighbor (kNN), maximum likelihood (ML), support vector machine (SVM), etc. However, frequency analysis typically need a high computational cost as well as a high sampling (or sensing) rate to affirm the performance and thus, a broader bandwidth network to transfer. That is why a new approach is needed in the area of sparse frequency. When all targets have their own inherent patterns, time series analysis can be an effective method for target classification with sparse sampling data in acoustic WSNs. A lot of research have been performed for this manner, mainly to retrieve some patterns in a large database or to do data mining [5][6][7][8][9]. However, the problem of time shifting and the problem of spatial variations caused by the strength of volume over different distances should be solved to apply the manner to WSNs.

In this paper, we assume the innate pattern of each target could be found, and we focus on target classification with the patterns using the Improved Derivative DTW-Cosine (IDDC) algorithm proposed as a new technique. Our data set are made by adding various effects to each original signal to emulate some distortion effects, and the performance is analyzed over volumes to consider the spatial variations. We first do preprocessing all data and make the reference model using the PAA (Piecewise Aggregate Approximation) [7] which draws the contour of each target. The input signal array is then used to get a similarity (correlation) for each reference by the proposed algorithm. Finally, the weak performances in lower and higher volumes are improved using a smoothing technique.

The rest of this paper is organized as follows. Section 2 contains a discussion of characteristics of acoustic signal in a sparse sampling WSN, and section 3 describes our algorithms. Our data collection and experimental setup are illustrated, and the performance of proposed algorithm is empirically compared in section 5. Finally, Section 6 concludes our experiments and discusses for future works.

2 Characteristics of Acoustic Signal in a Sparse Sampling WSN

We can see how much information of frequency remain in a sparse sampling WSN through looking into the spectrogram. The sparser sampled, the more smoothed with respect to frequency in the spectrogram of signal. Fig. 1 shows an example of aggravated spectrogram caused by sparse sampling. It is shown to be plain with respect to frequency, which means little frequency information is contained in the signal as a result of sparse sampling.

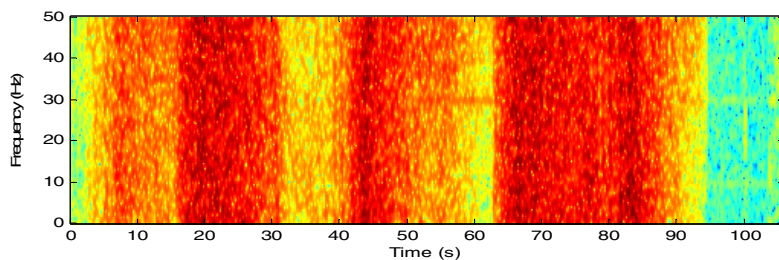


Fig. 1. Spectrogram of airplane signal sampled at 100Hz with 80points-STFT (Short-Time Fourier Transform), Hamming window and 90% overlap

As shown in Fig. 2, the shape of sampled signal can be different despite of being generated by the same target whenever sampled. It is because the sampling point of each signal differs from the others, which is one of the characteristics of WSN to make it more difficult to classify. To reduce the complexity of the signals, they are preprocessed as will be discussed in Sec 4.1. In addition, each signal not only is shifted with respect to time axis but also has different strength associated with the distance between the sensor node and the target in the field of WSN. So, we need a new algorithm which can solve the above problems efficiently.

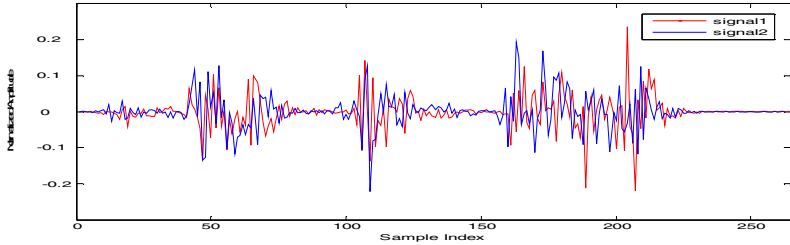


Fig. 2. Comparing two sampled signals made by different sampling points for the signal of airplane. Their shapes are different with each other.

3 Improved Derivative DTW-Cosine (IDDC) Algorithm

There are two problems, local time shifting and spatial variations, in applying the time series manner to the classification system of WSN. The first problem arises when a sequence is shifted or has different lengths from the other. It is solved by a time warping algorithm which uses dynamic programming. The other problem is caused by distance, which means that all the signals from the same object should be identified regardless of the strength of volume.

3.1 Time-Warped Algorithms

Three algorithms namely DTW [4], ED [5] and LCS [9] can be typically applied as a time warping algorithm. Table 1 shows comparing the core parts, distance function, of these algorithms. The DTW algorithm is frequently used to find the warped path through a matrix of points representing possible time alignments between two patterns. Given two time sequences, it fills an m by n matrix representing the distances of the best possible partial path using a recursive formula as its distance function in Table 1. The alignment that results in the minimum distance between the two sequences has value $D(m, n)$. To solve the problem of time scaling in time series, the DTW aligns the time axis and easily produces the matched array of time series in a well aligned manner. The ED, also known as the Levenshtein distance, between two strings is to find the minimum number of operations needed to transform one string into the other, where an operation is an insertion, deletion, or substitution. Lastly, the LCS finds the longest subsequence that two sequences have in common, regardless of the length and the number of intermittent mismatching symbols. However, the

performances of the LCS and the ED depend heavily on correct setting of the scaling threshold, which may be a particularly difficult problem for some applications as well as in WSNs.

Table 1. Comparing the time warping algorithms

| Name | Distance function |
|-----------------------------------|--|
| Dynamic Time Warping (DTW) | $D(i, j) = d(i, j) + \min \begin{cases} D(i, j - 1) \\ D(i - 1, j) \\ D(i - 1, j - 1) \end{cases}$ |
| Edit Distance (ED) | $d(x_i, y_i) = \begin{cases} 0 & \text{if } x_i = y_i \\ 1 & \text{if } x_i \text{ or } y_i \text{ is a gap} \\ 1 & \text{otherwise} \end{cases}$ |
| Longest Common Sub-sequence (LCS) | $d(i, j) = \begin{cases} 0, & \text{if } i=0 \text{ or } j=0 \\ d(i - 1, j - 1) + 1, & \text{if } i, j > 0 \text{ \& } x_i = y_j \\ \max[d(i, j - 1), d(i - 1, j)], & \\ & \text{otherwise} \end{cases}$ |

3.2 Similarity Measure Algorithms

The similarity measure algorithm is to measure the similarity settling the problem of spatial variations caused by distance. All signals from an object should be identified regardless of the strength of volume. The similarity can be measured with the degree of correlation or distance between two sequences. It can be reflected by the Euclidean, the Pearson [11], or the Cosine correlation algorithms described in Table 2 assuming that x' and y' is a matched array respectively.

Table 2. Comparing the correlation (similarity) measure algorithms

| Name | Distance function |
|-----------|---|
| Euclidean | $C(x', y') = \sqrt{\sum_{i=1}^N (x'_i - y'_i)^2}$ |
| Pearson | $C(x', y') = \frac{\sum_{i=1}^N (x'_i - m_x)(y'_i - m_y)}{\sqrt{[\sum_{i=1}^N (x'_i - m_x)^2][\sum_{i=1}^N (y'_i - m_y)^2]}}$ |
| Cosine | $C(x', y') = \frac{\frac{1}{N} \sum_{i=1}^N x'_i \times y'_i}{\ x'\ \times \ y'\ }$ |

To compare these algorithms with each other in WSN applications, suppose that there are three signals which have been collected on a BS in a WSN as shown in Fig. 3. y_1 and y_2 can happen when a moving object is varying in distance to sensor

nodes over time, which means a similarity measure algorithm should identify them. Referring to Table 3, the measures by the Euclidean algorithm represent distance values while the Cosine and the Pearson algorithms compute similarity. The more similar the signals are, the less is the Euclidean distance and the larger the measure of the Cosine and the Pearson similarities. The Pearson and the Cosine similarity algorithms identify y_1 and y_2 while the Euclidean algorithm can not classify them well. On the other hand, y_3 and the others may not be caused by the same object, which means they can be regarded as not exactly the same but similar. Table 3 shows that the Cosine similarity identifies minute differences while the Pearson similarity does not. An original signal should not be confused with the others to maintain the performance. That is why the former outperforms the latter. Consequently, we can say that the Cosine similarity can represent the characteristics of signal in WSN better than the others, which will be discussed in more details in Sec. 4.2.

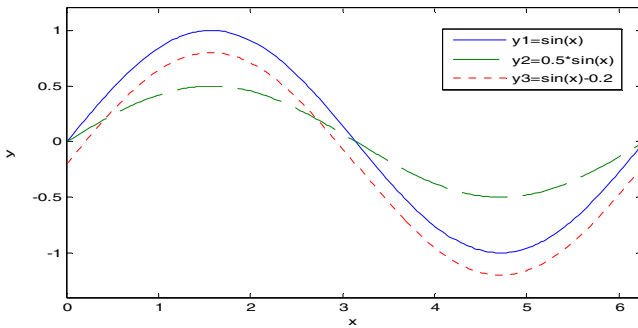


Fig. 3. Three signals that could occur in a WSN field

Table 3. The distance/correlation measures of three algorithms

| Algorithm | Euclidean | Pearson | Cosine |
|---------------------------|-----------|---------|--------|
| $y_1 \leftrightarrow y_2$ | 2.8025 | 1.0000 | 1.0000 |
| $y_2 \leftrightarrow y_3$ | 1.5875 | 1.0000 | 0.9622 |
| $y_3 \leftrightarrow y_1$ | 3.2211 | 1.0000 | 0.9622 |

3.3 Improved Derivative DTW-Cosine (IDDC) Algorithm

The IDDC algorithm combines the derivative DTW (DDTW) among variants of the DTW with the Cosine algorithm as the best classifier. The classic DTW algorithm has a tendency of producing unreasonable alignments where a single point in one sequence is mapped onto a large subsection of the other sequence when making a matching array (see the (a) of Fig. 4). It is because the algorithm finds an optimal path considering only the distance between a point of one sequence and its corresponding points of the other sequence. The problem led E. Keogh [6] to perform the DTW on the derivative of the time series instead of on the sequence itself. The (a) and (b) of Fig. 4 is to compare the results of the DTW and the DDTW. The DTW seems to fail to find the optimal alignment while the alignments produced by the DDTW look

better. However, the DDTW has a tendency of being more sensitive to noise than the DTW. So, E. Keogh [6] suggested the following estimate for robustness to outliers through simplicity and generality.

$$Q_i = \frac{(q_i - q_{i-1}) + ((q_{i+1} - q_{i-1})/2)}{2}, \quad 1 < i < m. \quad (1)$$

where q_i is a point of a sequence. Assume that the average m_N and the standard deviation σ_N of background noise are known, the estimate Q could be regarded as zero when $q \leq (m_N + \sigma_N)$ to avoid the influence of noise. The noise of background is mostly close to zero. In addition, the diagonal path $d(m-1, n-1)$ should be given the priority among the next paths not to lose the correct path when the next path will be found as described in (c) and (d) of Fig. 4. According to our experiments, this scheme should be considered especially for matching the points of background sounds. Finally, the Cosine algorithm measures the similarity with the array which this improved derivative DTW produced.

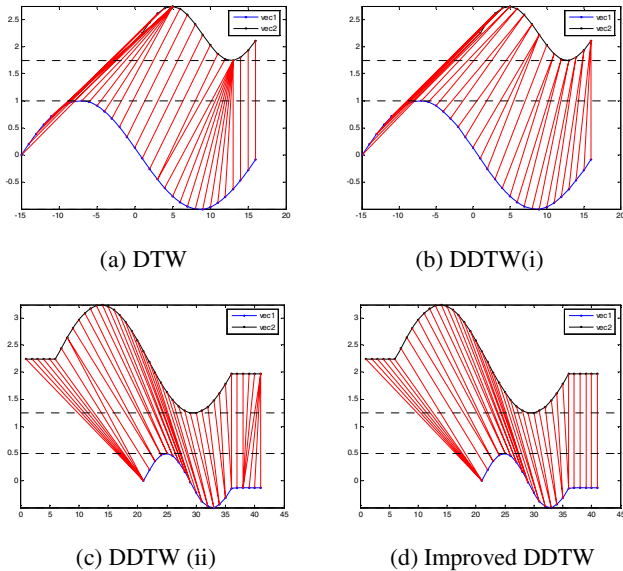


Fig. 4. Comparing the DTW, the DDTW, and the improved DDTW

4 Experiments and Evaluations

We first describe our experimental setup briefly, and the performances of the ED, the LCS, the DTW, and the IDDC are compared with each other. We then show the effectiveness of similarity measure algorithms through several experiments of the time-warped similarity measure algorithms including a smoothing technique.

4.1 Data Collection and Experimental Setup

Three types of military objects, airplane, tank and soldier, in Fig. 5 are classified in the experiment. As shown, the sound of a soldier is a step sound which is very periodic and the duration of local frame is very short while the sound of an airplane is sleek a little and has a long local frame. The tank makes the sound of irregular explosions against a background of the sound of engine and wheels, which has a monotonous energy. We added some effects and noise which produces some distortion to the signals, e.g. various Doppler effects, some hissing noises by size, echo, flanger, mechanize, pitch change, some volume transforming effects(fade in/out), and time warping. We made 31 test data per object and totally have 93 test data. Each file is sampled sparsely at 10 Hz 20 times and classified 1860 times against objects before obtaining the result.

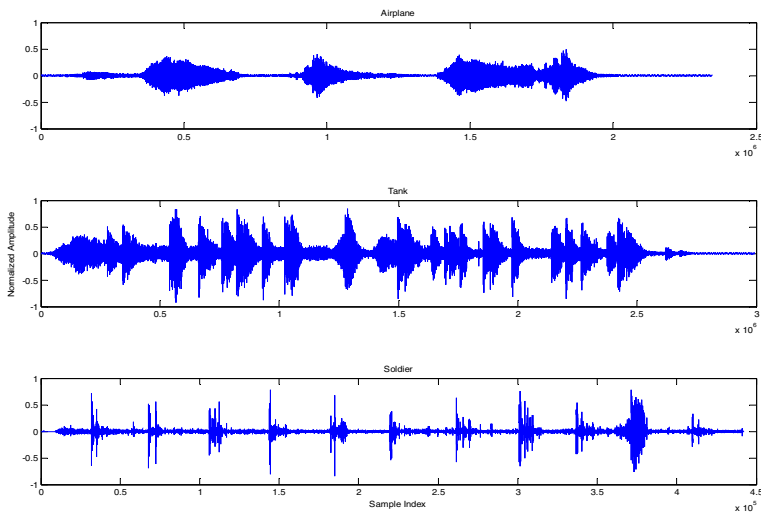


Fig. 5. Assumed signal patterns of military targets which can be occurred in a field of WSN

The overall experimental system architecture consists of preprocessing, making reference, and classification parts. First, in the preprocessing part, input signals are scaled between -1 and 1, and its absolute values are taken to reduce the variation and the computational complexity. Fortunately since they constitute the piecewise power values of symmetry at each point and are highly correlated with each other, the absolute values are very efficient without losing any information. Also, the smoothing technique is used to improve the accuracy in higher and lower volumes in this paper. It is computed by Eq. 2 assuming that N is the number of elements to smooth.

$$x_i' = \frac{1}{N} \sum_{j=i+1}^{i+N} x_j. \quad (2)$$

Second, to model the outline of the reference against the input signal, each reference signal is compressed to the length of input signal using the PAA technique, Keogh et al. [7] proposed, because each input has a different length case by case. The PAA compresses or models a signal as it draws the contour of the reference signal of an object as follows: Let N be the dimensionality of the transformed time series we wish to work with ($1 \leq N \leq n$). The i th element of is calculated by Eq. 3. Lastly, the signal is classified to the object category which has the best similarity caused by the time-warped similarity measure algorithm and the decision rule.

$$\bar{x}_i = \frac{N}{n} \sum_{j=\frac{n}{N}(i-1)+1}^{\frac{n}{N}i} x_j . \quad (3)$$

4.2 Comparison of Time Warping Algorithms

Before comparing the effectiveness of the three time warping algorithms, the ED, the LCS and the DTW, we experimented with the performance of the ED and the LCS with three levels of volume - half (-6.02dB), normal and double (6.02 dB) as shown Table 4. This is because the ED and the LCS should use a scaling threshold to apply to time series data, which consist of numeric values, and compare with the DTW. We explored the performance by varying the value of the threshold from 0.02 to 0.2. As shown in Table 4, the optimal threshold has a tendency to move following the level of volume. i.e., the threshold shifts to a smaller value in higher volume while it becomes larger in lower volume. While the optimal threshold comes to be 0.06 in double volume, it is 0.08 and 0.1 in normal and half volume respectively. Consequently, it is clear that the threshold cannot be easily established over volume.

Table 4. Optimal threshold of ED and LCS

| Volume level | ED | LCS |
|---------------------|------|------|
| Double Volume (6dB) | 0.07 | 0.06 |
| Normal Volume (0dB) | 0.08 | 0.08 |
| Half Volume (-6dB) | 0.1 | 0.1 |

The Fig. 6 shows the comparison of the performance of the time warping algorithms including the DDTW as well as the Improved DDTW (IDDTW). All of the DTW, the DDTW, and the IDDTW give a similar performance with the optimal accuracy of the ED and the LCS in normal and high volume and all of them have a poor performance in lower volume. It means that an algorithm which can improve the performance, especially in the case of lower volume, is needed. The IDDTW can not only produce a matching array with ease but is also superior to the DTW and the DDTW over all volumes. Consequently, it is reasonable that any similarity measure algorithm should be combined with the IDDTW to get the highest performance.

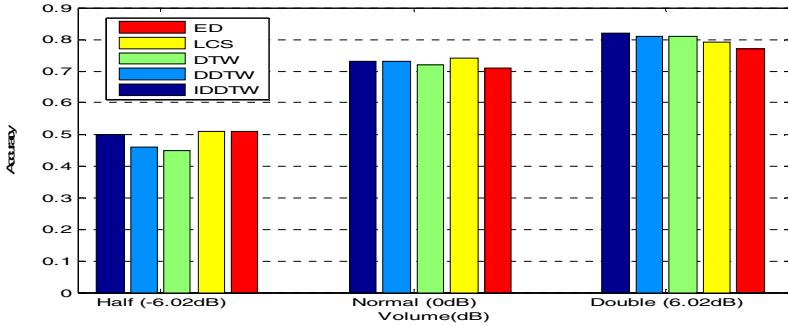


Fig. 6. Comparison of time warping algorithms

4.3 Comparison of Time-Warped Similarity Measure Algorithms Based on the IDDTW

We tested the IDDTW combined with all similarity measure algorithms as mentioned in section 3, and we found that the IDDC (IDDTW+Cosine) algorithm improves the performance in the area of lower volume very effectively and outperforms the other algorithms as depicted in Fig. 7. Although the performance of the IDDTW and the IDDE (IDDTW+Euclidean) algorithm shows a good performance from 5 to 8 dB, their performances are poor in lower volumes as well as have a tendency of degrading dramatically after 8 dB, which means they are highly dependent on the level of volume. On the other hand, the IDDP (IDDTW+Pearson) and the IDDC have saliently better accuracies in lower volume and are comparatively less affected by volume.

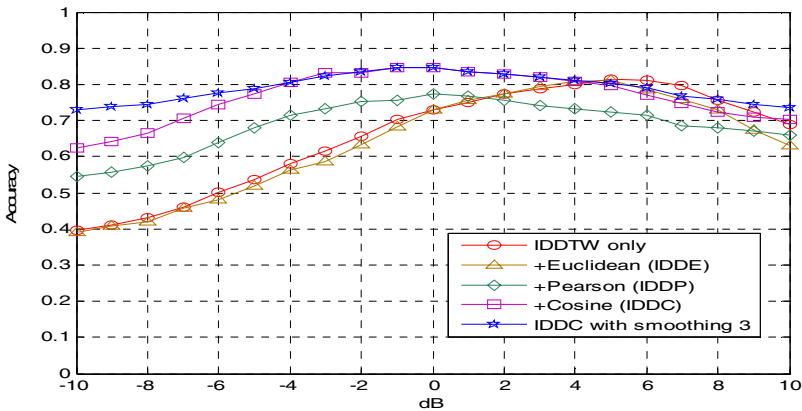


Fig. 7. Comparison of time-warped similarity measure algorithms

We experimented the IDDC algorithm + Gaussian smoothing which is helpful in improving the accuracy through avoiding distortions caused by odd elements. We

found the optimal number of elements for smoothing should be 3 through several experiments, so that the 3 elements came to be applied for smoothing in Fig. 7. Anyway, it turned out to be effective in improving the accuracy in both lower and higher volumes.

Table 5 shows the confusion matrix of targets corresponding to volumes. The accuracies of tank and airplane outperform soldier by and large because the width of pillars of signal from the soldier are so narrow that they are often unable to be sampled while the interval between them are so large that even skipping sampling once can be critical to the performance. The influence of volume is also shown to depend on the sort of sound. i.e. monotonous signals such as an airplane is affected negatively by strong volume while complicated and variable signals such as a tank is positively affected. It is because more monotonous signal is modeled relatively better in lower volumes than in higher volumes. Consequently Considering a range from -10 dB to 10 dB, the accuracy of the IDDTW is 65.35%, the IDDE is 63.77%, IDDP is 68.75%, the IDDC algorithm is 76.55%, and the IDDC algorithm with the smoothing technique 78.98% on the average. It means the optimized IDDC algorithm outperforms the other algorithms by at least 10.23%.

Table 5. Confusion matrix by the IDDC algorithm with the smooth3 technique corresponding to volumes

| Classified Object \ Volume | Volume | Soldier | Tank | Airplane |
|----------------------------|--------|----------------|----------------|----------------|
| Soldier | Half | 0.61335 | 0.23832 | 0.14833 |
| | Normal | 0.63748 | 0.20700 | 0.15552 |
| | Double | 0.52383 | 0.32384 | 0.15233 |
| Tank | Half | 0.09468 | 0.76488 | 0.14044 |
| | Normal | 0.01512 | 0.96205 | 0.02283 |
| | Double | 0.00463 | 0.99075 | 0.00462 |
| Airplane | Half | 0.01600 | 0.03681 | 0.94759 |
| | Normal | 0.00636 | 0.05602 | 0.93762 |
| | Double | 0.00512 | 0.14042 | 0.85446 |

5 Conclusion and Future Works

We described the characteristics of acoustic signals in a sparse sampling WSN and proposed the IDDC algorithm as the best classifier algorithm of time series. Since the acoustic signals not only comprise dense positive and negative values, but they also constitute the piecewise power values of symmetry at each point and highly correlated with each other, their absolute values and the smoothing technique are taken to improve the accuracy. Even though the experimental data are made artificially, it makes sense that the proposed algorithm has a satisfactory accuracy over volumes and outperforms compared to the other time-warped algorithms by at least 10.23% on the whole. We can also infer that the method of time series analysis can work collaboratively with the method of frequency analysis to operate a WSN economically. So, it is sure that our work could be a baseline for the research of target classification using the time series approach in the future.

Our future works will focus on applying physical features, the ZCR (Zero Crossing Rate), energy, etc, and multi-modal fusion to improve the accuracy since objects have different signatures from each other corresponding to multiple modalities, e.g. magnetic and seismic. The HMM (Hidden Markov Model) could also give us the capability to analyze more diverse, more general and longer signals.

References

1. Li, D., Wong, K.D., Hu, Y.H., Sayeed, A.M.: Detection, Classification and Tracking of Targets in Distributed Sensor Networks. *IEEE Signal Processing Magazine*, 17–29 (2002)
2. Meesookho, C., Narayanan, S., Raghavendra, C.S.: Collaborative classification applications in sensor networks. In: *Second IEEE Sensor Array and Multichannel Signal Processing Workshop*, pp. 370–374 (2002)
3. Duarte, M.F., Hu, Y.H.: Vehicle Classification in Distributed Sensor Networks. *Journal of Parallel and Distributed Computing* 64(7), 826–838 (2004)
4. Sakeo, H., Chiba, S.: Dynamic programming algorithm optimization for spoken word recognition. *IEEE Trans. On Acoustics, Speech and Signal Processing* 26, 43–49 (1978)
5. Chen, L., Ng, R.: On the Marriage of Lp-Norm and Edit Distance. *VLDB*, 792–803 (2004)
6. Keogh, E., Pazzani, M.: Derivative Dynamic Time Warping. In: *The First SIAM International Conference on Data Mining* (2001)
7. Keogh, E., Chakrabarti, K., Pazzani, M., Mehrotra, S.: Dimensionality Reduction for Fast Similarity Search in Large Time Series Databases. *Knowledge and Information Systems Journal* 3(3), 263–286 (2003)
8. Latecki, L.J., Megalooikonomou, V., Wang, Q., LakÅamper, R., Ratanamahatana, C., Keogh, E.: Partial Elastic Matching of Time Series. In: *Proc. of 5th International Conference on Data Mining*, pp. 701–704 (2005)
9. Guo, A., Siegelmann, H.T.: Time-Warped Longest Common Subsequence Algorithm for Music Retrieval. In: *IS-MIR. International Conference on Music Information Retrieval* (2004)
10. Chen, L., Åozsu, M.T., Oria, V.: Robust and Fast Similarity Search for Moving Object Trajectories. In: *ACM SIGMOD international conference on Management of data*, pp. 491–502 (2005)
11. Resnick, et al.: GroupLens: An Open Architecture for Collaborative Filtering of Netnews. In: *Proceeding of CSCW 1994* (October 1994)

Scriptable Sensor Network Based Home-Automation

Thomas Haenselmann, Thomas King, Marcel Busse, Wolfgang Effelsberg,
and Markus Fuchs

University of Mannheim,
A5, 6 · 68159 Mannheim · Germany
{haenselmann, king, busse, effelsberg,
fuchs}@informatik.uni-mannheim.de

Abstract. Today, proprietary home automation targets very specific applications which operate mostly on a cable based infrastructure. In contrast to that, our implementation builds a wireless ad-hoc multi-hop network based on the ESB sensor node platform from the FU-Berlin.

The nodes gather sensor readings in a home and transmit them to a central automation server. There, the readings are matched against a list of script statements. In case of a match, a specific action is performed. In this work we will show how the user can implement complex home automation applications optimized for his specific needs by defining very simple script statements. An important property of the system is also that the control of all home appliances is done by means of IR communication and Ethernet enabled multiple plugs. This way, the cooperation between manufacturers is no necessity in order to connect devices to the home automation network.

Keywords: home automation, building automation, sensor networks.

1 Introduction

While the field of RFID technology constantly produces new applications and solutions for real world problems, research on sensor networks tends to be a mostly academic topic in which strong commercial applications are still rare [15,9]. For this reason we want to describe a home automation project with sensor networks we have done in conjunction with Siemens Corporate Technology CT/SE2.

Home automation offers a not yet exploited degree of convenience, both for the private home and the office. Although the idea has been around for many years, the market can still be considered to be in its infancy. Today's home automation solutions are mostly proprietary. They usually target a small number of problems, such as satisfying security needs or the control of a limited number of devices, typically all from the same manufacturer. They operate based on a particular infrastructure, which requires extra cabling. So they are best suited for new buildings. They are limited to the applications a manufacturer offers.

The future proliferation of home automation will depend on its ease of installation. That is why we argue for wireless home automation. In addition, this might be the only solution for ex post installations and historic buildings which must not be remodeled. At the same time, we believe that an even more important aspect to making the smart

home a success will be to offer more freedom for a user to customize home automation application to his specific needs.

In short, the idea of our prototype is to gather all kinds of sensor readings in a home and forward them hop-by-hop to an embedded system to which we refer as the home automation server. Each time a new event is detected, the server runs over a list of script statements which can be defined by the user. In case of a match between the received event and the matching part of a statement, one or more actions are performed which can either be executed by the sensor nodes themselves or by multiple plugs which can be controlled via an Ethernet connection by the embedded home automation server itself.

The strength and contribution of our application lies in the combination of a larger number of sensor readings which allows to derive higher level semantics as compared to reacting on single sensor readings only.

In the following Section 2 we analyze today's existing standards in the field of home automation. In Section 3 we describe all technical aspects of our system and how to exploit multiple readings for concluding deeper semantics as compared to using single sensor readings, only. Section 4 concludes with an analysis of strengths and weaknesses of the system.

2 Related Work

Since the beginning of electrification, switching electrical devices has been done by means of connecting or disconnecting them to the power grid. In recent years, physically disconnecting a device from its energy source has become less popular. Instead, switching is done electronically. This means, that the inner device is separated from the switching circuit. As a consequence, the device can be powered on or off by a remote control. Some computer main boards even allow to react on network events. However, the downside is that the switching unit keeps consuming energy as long as it stays alert.

The changing paradigm in home automation is also that a device is no longer disconnected from the power grid. The function of the switch on the wall or even in the device is taken over by a network which is solely signaling events. The network which controls devices by transmitting datagrams is powered with a much lower current. The earliest instance of a pure datagram based network standard for building automation is the EIB standard implemented in 1992.

Even earlier home automation systems like the X10 system, combined the signaling network with the power grid. This technology denoted as *power-line* based has regained popularity recently as an alternative to DSL technology which requires dedicated signaling cables like telephone lines. On the other hand, power-line based systems have inherent problems like radio interference, security flaws and reliability issues which have never been solved completely.

2.1 Powerline-Based Home Automation Protocol X10

X10 is a power-line based building automation protocol. It is used to transmit the control signals via existing power lines without the need of dedicated signaling cables. X10 is used to trigger simple control events. However, it never gained a strong foothold for

mission critical applications because no feedback channel is provided and the effective data rates are only about 20 bit/s. The bits of a message are modulated on a 120 kHz signal. In order to be more error resilient, only the zero-crossings of the alternating current are used. In addition to the power-line based approach, X10 provides remote controls and switches based on radio communication, as well [14].

The X10 protocol was developed by the Irish company Mico Electronics in the 70ies. Due to its adoption and promotion by General Electric it became very successful in the United States. In Europe, a modified standard was sold which did not have the same success as compared to the one overseas. Due to different regulations, the signal strength had been reduced significantly thus rendering the solution less useful for many applications. As a consequence, the technically more advanced EIB protocol became dominant in Europe.

2.2 European Installation Bus (EIB)

As early as in the mid-80ies, different companies thought about using bus-topologies for home- and building-automation. Even at that time it was obvious that proprietary home automation solutions would hinder the proliferation of home automation. Leading manufacturers of electrical installation technology among them Siemens, Jung, Merten et al. founded the *European Installation Bus Association (EIBA)* in 1990 which became the *Konnex* association later. Their aim was to establish a joint standard for home automation [3,10,12]. This standard guarantees the interoperability of various devices and of systems like home appliances, air conditioning etc. from different manufacturers. In 1991, the first products were manufactured according to the standard. Today, there are as much as 4000 groups consisting of products manufactured by more than 100 companies. These products are compliant to the EIB/KNX specification which is the first globally agreed standard for home- and building automation. The standardization by the ISO committee is currently on its way.

2.3 KNX

KNX can be considered the international successor of the EIB standard. KNX is downward compatible to EIB and it has been acknowledged by more than 100 companies.

3 Scriptable Sensor Network Based Home Automation

Our system consists of the ESB [7] sensor nodes described in the next section. They transmit messages hop-by-hop over a tree topology which has to be initialized by the user semi-manually in advance. The root node is connected via its serial interface to the embedded home automation server described in Section 3.1. The embedded board runs a stripped down version of Linux and a minimal web server to allow the user to configure the system remotely.

The nodes not only act as sensors but also as actuators which can control basically all devices which come with an IR remote control. Therefore, we have extended the ESB's firmware to be compatible with the three de-facto standards for remote controls

by Philips, Panasonic and Sony. In addition, the buzzer and the LED lights can be used as actuators in some cases. More important is the multiple power plug with an Ethernet interface. It allows to switch all devices switch can be turned on and off only and which can not be controlled otherwise.

In the beginning, the nodes have to be distributed in the house according to the requirements of the considered applications. In the distribution process, the user is given hints by the system on where to place intermediate nodes for the purpose of communication.

In the operational phase, events are forwarded by the network to the root node and eventually to the home automation server in a tree-like fashion like it has been proposed e.g., by [8] in the context of the *TAG*-approach and may others [11]. There, they are matched against so-called script statements which have been configured by the user via a web-interface as described in Section 3.4. In case of a matching statement, a defined action is executed which implements one particular home automation application respectively which serves one particular purpose like e.g., baby surveillance. In this case, the executed action could be as simple as signaling the user with the buzzer or by sending him some information over the web by the embedded server, e.g., to submit an SMS via an external service.

3.1 Hardware Used

The electronic sensor board. Due to its rich instrumentation with various sensors we chose the ESB sensor node shown in Figure 1 developed by the FU-Berlin.

The ESB is equipped with the MSP430 [2], an embedded system on a chip from Texas Instruments. It runs at 8MHz and contains 64kB of memory in the version of the chip used here. The MSP430 is designed as a general purpose embedded system with a 12-Bit AD/DA (analog <-> digital) converter. The energy consumption is in the order of magnitude of 1mA at a current of 3V if the MSP430 is fully operational. In sleep mode which can be adjourned by external events, the power consumption is again about 1000 times lower which is roughly equal to the self-discharge of the batteries.

Most of the 64kB are implemented as flash memory which will contain the software and all constant data. The RAM occupies only 2048 bytes within the whole memory map which is a fairly limited amount of space for dynamic data. The situation is mitigated to a degree by the fact that the flash memory can also be written in chunks of 128 bytes during operation if the state of the battery allows for this energy consuming operation.

Under the ESB's white hemisphere are a temperature and PIR (passive infrared) sensor hidden. The PIR sensor can be used for monitoring the space around the ESB up to a distance of 8 meters to detect moving objects like it is used for alarm systems.

There are two other IR (infra red) diodes on the circuit board for sending and receiving e. g., RC-5 codes that are used by remote controls for consumer electronics. The IR-communication is particularly important because it allows the nodes to serve as actuators which can influence their environment by interacting with many home appliances like air conditions, home entertainment devices etc. At the same time the IR communication provides another way to influence nodes with consumer remote controls. They are treated like any other sensor event, sent to the embedded board and matched against a user-defines script statements.

Furthermore, the ESB is equipped with a vibration sensor that can sense slight vibrations of the device. Last not least, the ESB is equipped with a microphone and a piezo-electric buzzer. The buzzer is another simple actuator used to signal the user acoustically. By its design, it can only produce a single frequency, however, by switching it on and off rapidly, the firmware can also simulate other frequencies. There is also a microphone attached to the ESB. It can be used to measure the loudness of noises in the node's proximity. A very simple application would be to implement a baby-phone by signaling the owner in case of noise in the nursery.

The red, yellow and green LEDs are useful for signaling simple events. We use it in the deployment phase described in Section [3.5](#).

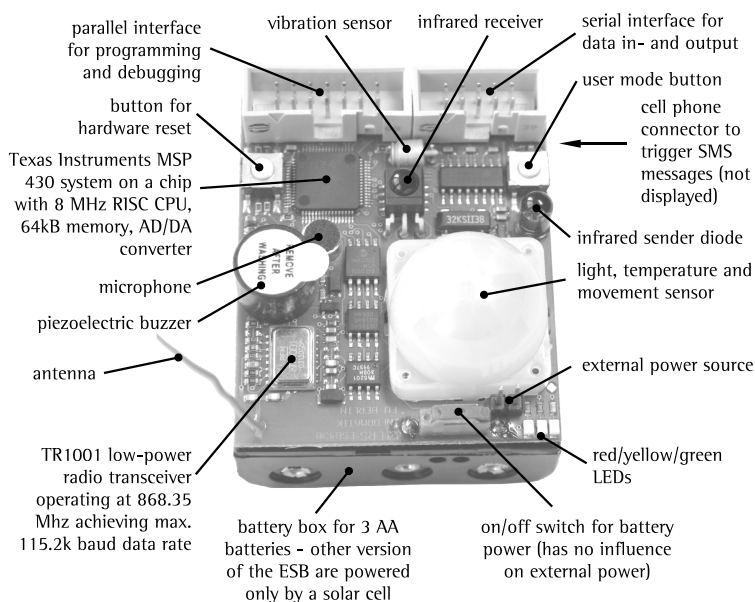


Fig. 1. Overview of the components of the Embedded Sensor Board (ESB) from the FU-Berlin

PowerPC-603 based embedded board. As what we refer to as a *home automation center*, we used the embedded board EP5200 from Embedded Planet. It is a complete system on a single motherboard. Though there is an IDE connector for a hard drive, we used the on-board 16MB flash memory for installing a minimal Linux installation based on the Linux distribution *Gentoo*. The flash memory can be accessed like a hard-drive using the *jffs2* file system.

Besides the need to cross-compile the kernel and to replace the hard drive by the flash memory, there is no different to using an IBM PC-compatible system. However, it is important to delete all files not needed in the boot process to achieve a memory footprint which fits into the bounds of the 16MB flash memory. In the development process we attached a simple USB stick to the USB port to host the GNU tool chain and other essentials.

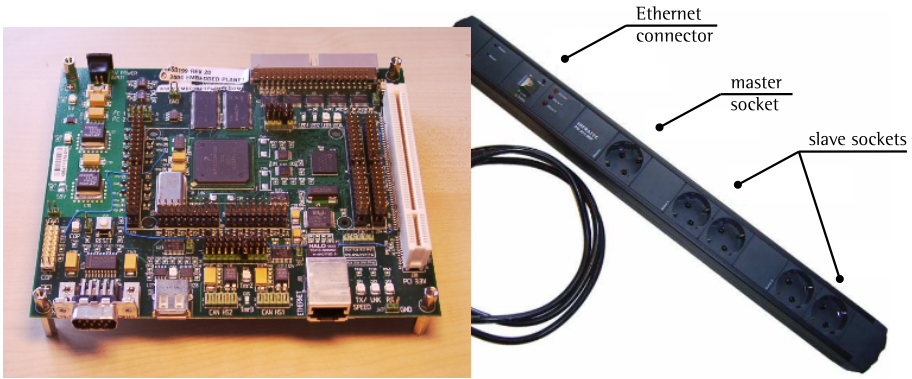


Fig. 2. The EP5200 board is based on an PowerPC-603 processor. It has no moving parts. The flash memory can be used to host the root file-system.

We believe that an embedded system is suitable for its small form factor, price and stability. It has no moving parts, needs no ventilation and is certified for continuous operating in an environment of between -40 to 80 degrees Celsius.

Ethernet-enabled multiple plug. An important actuator is the ethernet-enabled multiple plug shown in Figure 2. It can be used to switch all electric equipment which has an on/off switch only like e.g., lamps. From a user's perspective, the multiple plug can be controlled via a web-interface. In our implementation, the home automation center sends simple http-requests to the socket in order to switch one of the two relays on or off.

The downside of the solution is so far, that the multiple plug needs to be connected to a cable-based LAN. However, we expect similar wireless devices to be available soon as well. As an intermediate solution we connected an Ethernet bridge to the plug in order to become independent of the LAN-cable.

The master socket can be used to switch one or the two slave sockets on if the attached master device consumes energy. At the moment, we control the slave sockets via Ethernet only.

3.2 New Home Automation Paradigm

Traditional home automation solutions target isolated problem. They may e.g., close the window's roller blinds at night, control the central heating and air conditioning or they may serve security needs.

Some solutions are helpful for handicapped people. If the doorbell or the telephone can not be heard, sensors capture the acoustic signals and trigger actuator like spot lights or vibrating haptic devices which wake or signal the hearing impaired owner.

In recent years, even solutions for pet owners have emerged. A cat's collar is equipped with a passive RFID transponder. At the cat door, a reader reads the passive tag within a range of about 30cm. Once the cat approaches the reader and the tag

is authenticated, the door is unlocked by a simple mechanism. This way, alien cat, rats or other small animals can be prevented entry from the house.

All those solutions have in common, that they target a very specific application only. Especially those for disabled people can be very costly and may not always solve all individual needs. So we propose a new paradigm which enables the user himself to devise customized solutions by means of simple script statements.

3.3 User-Define Home Automation Scripts

In the home automation center, all sensor readings are gathered. The user defines script statements like the following one which are matched against the incoming sensor readings.

```
IF movement_detected(sensor-5) == true THEN
    switch_power(multi_plug-5, on),
    switch_power(multi_plug-6, on)
```

Every script has a *matching part* and an *actuator part*. The server software on the home automation center iterates over all script statements each time an event is received. In case of a match, the actuator part is executed.

The above example switches on two lamps connected to a multiple plug outlet each time a room is entered by a person. Besides these trivial statements, the strength of the approach lies in the combination of more than one sensor readings. The more readings are combined, the higher the semantics that can be derived.

The example above could be extended by the time of day to differentiate between various situations. E.g., switching on the light is not necessary at any time but only at dusk or at night. So we add a light reading on the matching side:

```
IF movement_detected(sensor-5) == true AND
    lightness(sensor-5) < 800 THEN
    switch_power(multi_plug-5, on),
    switch_power(multi_plug-6, on)
```

Not all events have to be triggered by sensors. Another independent event can be the daytime.

```
IF time_within(05:00,23:00) == true AND
    movement_detected(sensor-5) == true AND
    lightness(sensor-5) < 800 THEN
    switch_power(multi_plug-5, on),
    switch_power(multi_plug-6, on)
```

```
IF time_within(23:00,05:00) == true AND
    movement_detected(sensor-5) == true THEN
    switch_buzzer(senor-7, on)
```

In the first line, a movement at daytime causes a light configuration to be switched on. In the second line, the same movement will trigger an alarm if it occurs while the owner sleeps at night.

A word on an implementation issue: Most sensors of the ESB motes sample measurements all the time which may even be noise in case of silence. In order to trigger e.g., an audio event or a moment event, the platform's firmware allows to specify threshold values for various sensors. Once these thresholds are exceeded, a message is sent out. Alternatively, the raw values can be sent via the wireless interface, constantly. This option is less popular for its high energy consumption. Setting thresholds, however, requires some prior configuration of the nodes within their particular environment.

Another example for deriving higher level semantics from sensor readings is shown in our demo-video¹. One of the ESB sensor nodes is attached to a door facing the inside. Two different readings are transmitted by the sensor, one originating from a passive infrared movement sensor that detects movement in a proximity of about 8 meters. The other reading comes from a vibration sensor which detects if the sensor itself is shaking. The two sensor readings can be used to differentiate between a door being opened from the inside or outside. To be more precise, the order of occurrence determines the case.

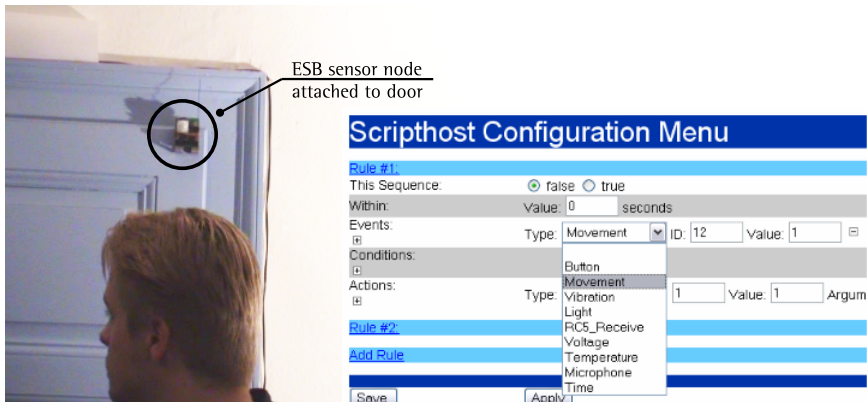


Fig. 3. Extract from our demo video: Two sensor readings are used to distinguish whether the door is approached from the inside or the outside (left). Browser-based configuration (right).

Door being opened from the inside: Here, a person approaches the door respectively the attached sensor node. The passive infrared sensor will trigger an event which is sent to the embedded home automation center. Then, the person will open the door which triggers the vibration sensor in addition because the entire node is moving together with the door.

Door being opened from the outside: A person approaches the door from the outside. No sensor readings are triggered so far because the sensor is attached to the opposite side. Once the door is opened, both sensors react at the same time. The vibration sensor because it is moving together with the door and the passive infrared sensor because it is rotated by the opening door. Move precisely, from its perspective, the environment rotates around the node. So both events occur more or less simultaneously.

¹ See http://www.informatik.uni-mannheim.de/~haensel/sn_homeautomation.avi

But not only taking multiple sensor readings into account at a time can help to derive higher level semantics. Historic events can help as well.

Example: We assume that a house is empty in an initial state and no door has been opened so far. If movement occurs in a room, someone may have entered through a window. If there was prior movement in the hall or the door has been opened it may be an inhabitant. Historic events are modeled by conditions which are described in the next section.

The examples above should only provide a first impression of the possibilities which emerge if many sensor reading are gathered and matched in order to draw conclusions. These conclusions can be far more valuable than those which are derived from single sensor readings as done in many isolated home automation applications. In this work we only want to sketch the idea of customized home automation and prove its feasibility by means of the implementation. As is true e.g., for the World Wide Web as well, the most interesting applications will likely come from creative practitioners and not from academia.

3.4 Web Configuration of Rules

Figure 3 (right) shows the browser based configuration. The user can define an arbitrary number of rules each of which appears as a single line that can be unfolded to a dialog for later editing.

A rule consists of three elements whereas the triggering event and the action to be performed are the two compulsory elements. Whenever an event like a sensor reading occurs, it is compared with all rules. If the event matches a rule, the according action is performed.

Whether an action is performed must not always depend on an event only but also on a condition which, unlike the event, persists over some time and does not occur at a single moment only. So a rule can have an arbitrary number of conditions which have to be met in addition to an occurring event. A condition can e.g., be a specific time of the day or a prior sensor reading like light or temperature. Multiple events, conditions and even actions can be defined within a single rule by the user. This way, the above mentioned deeper semantics can be accomplished.

Technically, the page is generated by a php-script on the server side and the rules are stored in a single XML file.

3.5 Deployment Phase

Prior to the operational phase of the home automation network, the sensor nodes have to be deployed. In the beginning, the root node and the leaf nodes have to be installed. The root node has to be connected to the embedded board which should have access to the home's LAN. The LAN connection is mainly used to control the Ethernet enabled multiple plug that is used to switch simple electronic devices on and off.

The location of the leaf nodes is determined by the purpose of the application. If the audio-sensor should e.g., be used as a baby-phone, a sensor node has to be positioned in the nursery. The root node and the leaf nodes are considered as *active nodes* in our implementation because they server a specific purpose. Especially in an indoor environment, the range of the sensor nodes can be limited, particularly if neighboring nodes are

separated by walls. So direct communication between leaf nodes and the root can not be assumed in general. This is why the user has to bridge the gaps between the root and the leaves by positioning intermediate *passive nodes* which server as packet forwarders only.

All nodes connected to the root directly or indirectly are considered to belong to the *active partition*. The task of the user is now to connect the active partition to all leaf nodes which are unconnected. In the deployment process he picks up initialized nodes and carries them away from the active partition into the direction of a leaf nodes. While being close enough to a connected node of the active partition, the green LED is blinking to indicate a good connection. It is considered to be good as long as three consecutive ping packets return from the root node. Less than three packets result in a yellow indicator and no arriving ping packets are signaled red. The relatively small number of test packets has been used because each of them takes about 300ms to be transmitted. A latency of about 1s is still small enough as feedback for the user.

So he will start at the active partition and walk towards a yet unconnected leaf node. As soon as the quality of the connection decreases, he has to step back and position the nodes permanently. In the end, the node is put into its operational mode by pressing the user definable button. The leaf node will also try to reach the active partition by sending broadcast ping packets. As soon as there is a good connection it will start to blink green as well and can be set into the operational mode in the same way as the nodes carried around. The user has to continue this process until all leaf nodes are connected. Note that in some cases, active nodes can and will serve as forwarders also if they are connected to the active partition themselves. The routing of the packets among the nodes is done according to the tree which is generated by the user implicitly by deploying the nodes. As a consequence, each node forwards information only to its direct father via static routes. Gathering the sensor readings was also easy to implement on the side of the nodes as the firmware readily supports sending events in regular intervals and based on thresholds.

4 Evaluation

In the evaluation, we mainly focused on a qualitative analysis of our implementation since there were not prior wireless home automation systems available to us.

4.1 Energy Supply

Even though the use of sensor nodes eliminates the need for cables, it creates the new problem of supplying the nodes with energy. Even under optimal conditions, our ESB motes will not operator more than a couple of months on a single set of batteries. Having 20 or more nodes installed, this would mean for the user to change some batteries once in a week on average.

The ESB nodes come in different versions. One of them replaces the battery box by a photo diode which charges a capacitor. Depending on the light conditions, the energy stored this way is enough to operate for a few seconds. Though this does not seem to be much, for many applications it suffices for making some measurements

and sending them over the network. Often, this does not require more than several hundred milliseconds. A useful property for the ESB platform is in this context that sensor readings can be used to wake the node from its power saving mode without using the processor. Waking up a node means to raise the clock rate of the processor which can e.g., be triggered by defining a threshold for a sensor. Though the threshold is a simple means of measurement it is useful for saving energy in times of inactivity.

At a first glance, intermediate nodes must not sleep since they may have to forward packets from their neighbors at any time. However, a number of MAC schemes like *WiseMAC* have been developed in recent years which keep a network alert while almost completely reducing idle times [6][13].

4.2 Security Problems

Wireless transmission is known to be error-prone in general and in particular in case of many sensor nodes. We exemplarily evaluated the transmission characteristics of our sensor platform [5]. One outcome of the studies was that there is a very strong variance both in transmission and reception characteristics among different nodes of the same type [4]. Furthermore, the quality of a directed link between two nodes can deviate significantly from the inverse direction.

Another problem which is inherent to all wireless networks is that it can be sabotaged easily by jamming the frequency band used. So the wireless channel is more useful for less mission-critical applications. In case of an alarm system, a beacon based approach might be adopted. The alarm could be triggered by missing beacons so that distorting the channel would not prevent the alarm. Though less critical, an attacker could still trigger false alarms.

On the other hand, the use of wireless communication is more and more debated, e.g., for industry automation [16] and even for communication within airplanes. The later one is referred to as *fly-by-wire*. First prototypes have been built based on unmanned planes [1].

5 Conclusion and Outlook

In this work we described a wireless home automation system based on sensor networks. The ESB platform we chose allows for easy installation and extension of the system.

Other than commercial home automation solutions available today, we propose to let the user come up with customized solutions for his individual requirements by formulating script statements. These statements which are entered via a web interface react on a combination of events and can trigger a list of actions in case of an occurring match. Furthermore, the execution of the actions can be made dependent on an arbitrary number of conditions which have to be met.

The nodes do not only act as sensors but as actuators as well. By sending infrared RC5 codes, almost all electronic equipment using a remote control can be switched. Simple devices are switched by means of a multiple plug with an Ethernet connection.

Though an increasing number of home appliances are controllable by IR remote controls today, we plan to connect to the European Installation Bus in addition. In this context it will make sense to adopt the EIB protocol for the wireless communication as well, at least on the application level. The extension of EIB to a wireless implementation could work in the style known from the Bluetooth standard. There, the layer two serial line connection is emulated by an underlying wireless connection. The actual application level communication does not have to be changed. In our case we aim at running the EIB protocol on top of the wireless connection in the next version of our prototype.

References

1. Afonso, J.A., Coelho, E.T., Macedo, R., Carvalhal, P., Silva, L.F., Almeida, H., Santos, C., Ferreira, M.J.: A fly-by-wireless platform based on a flexible and distributed system architecture. In: *EEE International conference on industrial technology*, Mumbai, India (2006)
2. Bierl, L.: *Das groe MSP430 Praxisbuch*. Franzis Verlag GmbH (2004)
3. Bruegge, B., Pfluegar, R., Reicher, T.: Owl: An object-oriented framework for intelligent home and office applications. In: Streitz, N.A., Hartkopf, V. (eds.) *CoBuild 1999*. LNCS, vol. 1670, Springer, Heidelberg (1999)
4. Busse, M., Haenselmann, T., Effelsberg, W.: The Impact of Resync on Wireless Sensor Network Performance. In: *PWSN 2006*. Wireless Sensor Networks, Coimbra, Portugal (2006)
5. Busse, M., Haenselmann, T., King, T., Effelsberg, W.: The Impact of Forward Error Correction on Wireless Sensor Network Performance. In: *RealWSN 2006*. Proc. of ACM Workshop on Real-World Wireless Sensor Networks, Uppsala, Sweden (2006)
6. El-Hoiydi, A., Decotignie, J.-D., Enz, C., Le Roux, E.: Wisemac, an ultra low power mac protocol for the wisenet wireless sensor network. In: *Proceedings of the 1st international conference on Embedded networked sensor systems*, pp. 302–303. Los Angeles (CA) (2003)
7. Kappe, E., Liers, A., Ritter, H., Schiller, J.: Low-power image transmission in wireless sensor networks using scatterweb technologies. In: *Workshop on Broadband Advanced Sensor Networks*, San Jose (CA), USA (October 2004)
8. Madden, S., Franklin, M., Hellerstein, J., Hong, W.: Tag: a tiny aggregation service for ad-hoc sensor networks. In: *Proceedings of the OSDI 2002 Symposium*, Boston (MA), USA (December 2002)
9. Orr, R., Abowd, G.: The smart floor: A mechanism for natural user identification and tracking (2000)
10. Pitzek, S., Elmenreich, W.: Configuration and management of a real-time smart transducer network (2003)
11. Singh, S., Woo, M., Raghavendra, C.S.: Power-aware routing in mobile ad hoc networks. *ACM SIGCOMM Computer Communication Review* archive 28(3), 5–26 (1998)
12. Spinellis, D.: The information furnace: User-friendly home control. In: *Proceedings of the 3rd International System Administration and Networking Conference SANE 2002*, pp. 145–174 (2002)
13. van Dam, T., Langendoen, K.: An adaptive energy-efficient mac protocol for wireless sensor networks. In: *Proceedings of the 1st international conference on Embedded networked sensor systems*, pp. 171–180. Los Angeles (CA) (November 2003)

14. Wang, Y., Russell, W., Arora, A., Jagannathan, R.K., Xu, J.: Towards dependable home networking: An experience report. In: DSN 2000. International Conference on Dependable Systems and Networks, p. 44 (2000)
15. Want, R., Fishkin, K.P., Gujar, A., Harrison, B.L.: Bridging physical and virtual worlds with electronic tags. In: CHI, pp. 370–377 (1999)
16. Wiberg, P.-A., Bilstrup, W.: Wireless technology in industry-applications and user scenarios. In: 8th IEEE International Conference on Emerging Technologies and Factory Automation, vol. 1, pp. 123–131. Antibes-Juan les Pins, France (October 2001)

Applying Situation Awareness to Mobile Proactive Information Delivery

SuTe Lei, Kang Zhang, and Edwin Sha

Department of Computer Science, The University of Texas at Dallas,
Richardson, TX 75083-0688, USA
sute@acm.org, {kzhang, edsha}@utdallas.edu

Abstract. Proactive information delivery systems disseminate information to users based on their current tasks. Interests for proactive information delivery to mobile users are growing. In a mobile environment, users have access to additional ambient information that is not usually present in a fixed working location. It provides an opportunity to improve the quality of information delivery service by utilizing ambient information. However, mobile users tend to be distracted by their surroundings. Ideally, the information delivered to mobile users should match with their current tasks and needs. The challenge is how to determine users' needs. We tackle this issue by analyzing users' responses to delivered information and learning from their perceptions towards situations. This paper presents an interval-based approach for situation specification. We show a prototypical system that uses the reinforcement learning technique to obtain better understanding of users' perceptions towards situations.

Keywords: visual specification, situation awareness, proactive system, reinforcement learning, interval algebra.

1 Introduction

Proactive information delivery is a software service that delivers information to users based on their current tasks. Typical examples are systems like Amazon.com's associated product recommendation and Google's AdWords advertising. Today's advanced mobile technology enables users to gain access to information ubiquitously. Unlike the user using a stationary desktop computer, mobile users have more choices of information access such as mobile phones, UMPCs and PDAs. The mobility nature provides proactive computing an opportunity to improve the quality of information delivery by identifying users' locations and their current tasks via pervasive or ubiquitous computing services. In a pervasive computing environment, additional ambient information is made available for more accurate detections of the user's current context. It thus facilitates a better quality of proactive information delivery service. However, there are some challenges in delivering information to mobile devices. First, mobile devices have limited resources, e.g., CPU power, display size and memory space. Input techniques are also different. Second, the ambient environment is more dynamic. Users might be on the subway train or in a shopping mall while using the

system. The possibility of being distracted by the surroundings is high. As pointed out by Chittaro [4], in mobile situations, using the device often becomes a secondary rather than a primary task. Proactive information delivery might result in being intrusive to mobile users. Thus, we must take extra measures when migrating proactive services from desktop operating environments to mobile ones. In addition, the precise meaning of a situation is vital for determining the contents to be delivered to mobile users. A specification method is needed to achieve this.

In order to provide proactive services, we apply the concept of situation awareness to improve the appropriateness of information delivery. The notion of situation awareness as defined by Endsley [5] is the perception of the elements in the environment within a volume of space and time, the comprehension of their meaning and the projection of their status in the near future. We present our idea based on Endsley's definition that encompasses the notion not only on spatial aspect of the perceived information but also the temporal constraint which might have an impact on users' tasks. We begin the discussion by reviewing related work in section 2. Section 3 describes our specification method. In section 4, we discuss the issues in applying situation awareness and propose a prototypical system. We conclude our discussion in section 5. The contributions of our work are twofold:

- we propose a specification approach using interval algebra to model situations.
- we implemented a prototypical proactive information delivery system that employs a reinforcement learning technique to understand users' perceptions towards the delivered information.

2 Related Work

The key feature of proactive information delivery systems is the ability to provide information based on the detected user needs. In the literature, the capability is often referred as context awareness. A plethora of context-aware systems have been proposed in recent years. Due to space limitation, we limit our discussion to those systems that are closely related to proactive systems and systems employing the concept of situation awareness.

Yau and Liu [10] proposed an approach to incorporate situation awareness in service specification for situation-aware service-based systems using SAW-OWL-S, an extension of OWL-S with situation ontology. They presented a method to identify the relationship between situations and services in situation-aware service based systems. We share a similar view with their work that situation specification plays an important role in system developments. The Watson system [3] is an information management assistant system that observes user interactions with everyday applications, anticipate information needs, and automatically fulfill them using Internet information sources. A query in Watson is grounded in the context of the user's tasks. The system turns everyday applications into intelligent, context-bearing interfaces to conventional information retrieval systems. The FXPAL Bar system [2] is a proactive information recommendation system designed to provide contextual access to corporate and personal resources. It enhances information recommendations by adding three features - *translucent recommendation windows* in the program interface which increases the user's awareness of particularly highly-ranked recommendations, *query term*

highlighting that communicates the relationship between a recommended document and the user's current context, and a *recommendation digest* function that allows users to return to the most relevant previously recommended resources. The TaskNavigator system [7] improves the reuse of previous process know-how by proactively suggesting similar tasks or relevant process models based on textual similarities. It uses the functionality of the commercial system, BrainFiler, to find similar document categories. The system allows the user to build a personal knowledge space. The concept is similar to the use of user profile.

One of the earlier systems using the user profile approach is the Letizia system [8]. It uses implicit feedback such as bookmarking, to learn a user profile. It performs lookahead search in the locus of the page the user is currently viewing and recommends links accessible on the current page. Many other related work using recommendation agents to improve information retrievals can be found in Greengrass's survey [6]. Our work differs from previous approaches in that we focus on the aspect of data representation and information delivery services to mobile users.

3 Situation Representation

A situation is a finite sequence of actions as defined in situation calculus [9]. In our view, a situation is a result of an orderly combination of actions that occur over a finite interval of time. We use a four-layer model to represent situations – data atom, data element, data transition and situation. The data atom layer contains low-level data obtained directly from data sources. On top of the data atom layer is the data element layer. Data elements are fusions of data atoms. The next level is the data transition layer which specifies the actions performed on data elements. The top level is the situation level which defines situations using a combination of actions. The data components at the four layers are described in table 1.

Each data atom has five main attributes - name, value, value type, timestamp, and data source. The sources of data atoms could be one of the followings:

- raw data from sensor systems such as temperature, humidity, and noise level
- data feeds from web services such as up-to-the-minute financial and weather data
- message notification such as mobile phone's SMS messages and emails

A data element is an interpreted piece of information inferred from data atoms. Each data element is defined by its name, an element type, a set of data atoms, an interpretation function, and a list of interpretations. For example, we may define a data element indicating three degrees of comfort level (cold, pleasant, humid) of a meeting room by setting the readings from its room temperature and humidity. We may also define an email filtering function that serves as a rule to process the content of a data atom pulled from an email box, and the data element being defined is assigned with an email category which allows an email program to perform further processing.

As mentioned above, a situation is an orderly combination of actions. An action is the fact or process of doing something. From the system perspective, we want to be able to reflect this fact in a way that the system can utilize it for further processing. In real life, an action spans over an interval of time despite the granularity of the interval. For example, the declining process in a particular stock from \$35.8 to \$32.2 from

10:00 AM to 11:00 AM. The process may be caused by a variety of reasons. In a situation-aware environment, the causes for any change in data value are quite often unknown. To capture the act of a process, we thus pay attention to the consequential effect of an action, that is, the state change of a data element. We use *data transition* to represent the effect of an action and define it as a process spans over an interval marked by a begin state and an end state (see Table 1). Since actions are treated as an interval, we need to consider the temporal relations among them. According to Allen's interval algebra [1], seven basic possible relations between two distinct intervals

Table 1. Definitions of data components

| Data component | Description |
|-----------------|---|
| Data atom | A low-level data unit obtained from a data source by data pushing or pulling. |
| Data element | A data element is $e = (A, f)$, where A is a set of data atoms and f is an interpretation function that maps the combined values of A to a list of interpretations. |
| Data transition | A data transition is $t = (ei, vi, ve)$, where vi is the initial value of a data element or elements ei with the element type i , and ve is the ending value of ei . |
| Situation | A situation is $S = (T,R)$, where T is a set of data transitions, and R is the relations among I . The possible relations are <i>before</i> , <i>meets</i> , <i>overlaps</i> , <i>starts</i> , <i>during</i> , and <i>finishes</i> . |

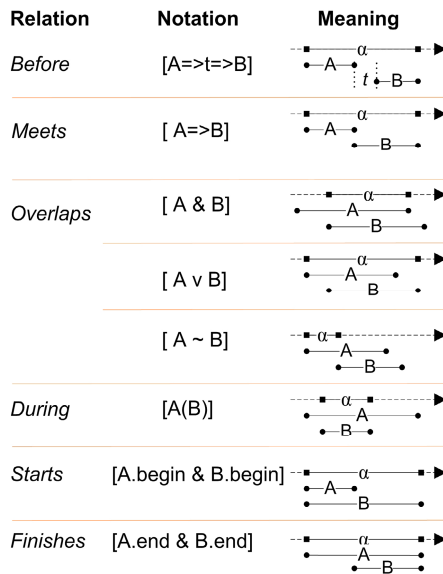


Fig. 1. Temporal relations of data transitions. The set of operations of two distinct data transitions, their notations, and temporal meanings. The value of α is evaluated to true if the relation condition is met.

exist – *before*, *meets*, *overlaps*, *starts*, *during*, *finishes* and *equals*. We developed a set of notations for specifying situations based on these terms. Basically we specify the begin and end of a data transition by adding two suffixes at the end – *begin* and *end*. For example, *StockRise.begin* indicates the begin of *StockRise* data transition. Fig. 1 depicts the relations and our notations. We left out the *equals* relation as it is not used in our context.

By using an interval-based approach as opposed to a point-based one, we are able to more intuitively represent situations and perform queries on them. For example, suppose we have the following two actions:

A1: Tom enters through the building entrance.

A2: Tom is in a meeting.

A1 normally occurs and ends in just few seconds, whereas the duration of A2 is usually longer than 2 minutes. We may determine if Tom is still in the meeting by checking the existence of A2. We may also check if Tom is in the building by checking if A1 has occurred. The difference here is in the time of checking. We check the status of A2 while A2 is still happening, and we are only interested if A1 has occurred.

4 A Situation Aware Proactive Information Delivery System

The concept of situation awareness has long been used in mission-critical information systems such as military and disaster control systems. There are basically three levels of awareness - perception of elements in current situation, comprehension of current situation, and projection of future status. Working memory and attention are the two key factors that influence the accuracy and completeness of situation awareness. The way in which attention is employed in a complex environment with multiple competing cues is essential in determining which aspects of the situation will be processed to form situation awareness [5]. We must take these factors into consideration when applying situation awareness to proactive information delivery services. In the subsections below, we will firstly discuss the method for discovering situations and assisting situation comprehension and projection. We then propose a prototypical system based on the methods discussed.

4.1 Situation Awareness

The goal of applying the concept of situation awareness to proactive information delivery systems is to improve the appropriateness of the delivered contents. One of the key aspects in situation awareness is that it is a cognitive process of continuous adjustments in the user's perception and comprehension towards a situation. The task is not merely identifying the current situation of a user, but also continuously monitors the implication of the detected situation to the user's perception. From the system perspective, we need a way to discover how a user perceives a detected situation. It thus requires a mechanism that enables the system to learn from users' actions and adjust the delivery policy accordingly.

Among several types of machine learning techniques, reinforcement learning best suits our goal. It differs from supervised learning in that correct input and output pairs are never presented, nor sub-optimal actions explicitly corrected. It tries to find a balance between exploitation of current knowledge and exploration of uncharted areas. To apply reinforcement learning into our system, we have the following setup:

- specify a set of situations for triggering information deliveries
- define a discrete set of environment states
- specify a discrete set of actions
- define a set of scalar rewards for the set of environment states.

Upon a situation detection, the system sends out information to its users. When users receive the information, they have few options to respond. The system registers each response and calculates the reward. Based on the calculated reward value, the system adjusts the delivery policy for the next delivery. The goal is to find an optimal delivery policy, mapping states to actions, that maximizes a long-term reward value. Fig. 2 illustrates the process.

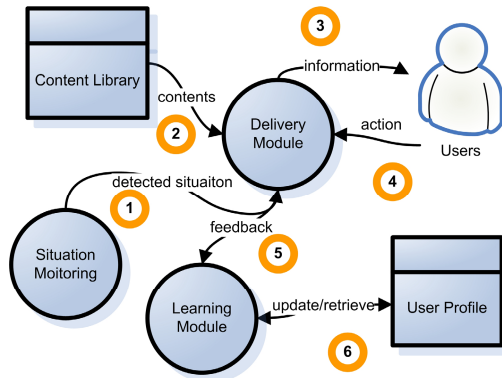


Fig. 2. The reinforcement learning process. A detected situation is processed by the delivery module which chooses an appropriate delivery policy and data contents from the content library. This information is then disseminated to users. Responses from users are fed back to the learning module. The learning module registers users' actions and calculates the reward values and stores the data into the user profile. Updated information contents are sent to users. Depending on the information content, the process can be repeated until the interaction session ends.

As the interactions between users and the system are open, the learning process can take an indefinite period of time to converge. For example, suppose that we have a set of recommended contents and a series of steps for users to follow. Depending on users' actions, predefined recommendations will be sent at each step. When a user receives a pushed content, he/she may or may not reply. In addition, we do not know if the user will follow through the preprogrammed steps, and we do not know when the user will respond to the delivered contents. The user might stop using the system at any point due to a variety of reasons. As a result, the learning task becomes an ongoing process. In some cases, such as interactive advertisements, immediate or

short-term learning results are required. One way of forcing the system to obtain a final reward value is to impose a time constraint or to limit the number of interactions. It can be specified in each delivery policy. In next section, we will describe a prototypical system based on the concept discussed.

4.2 A Situation Aware Proactive Information Delivery System

We implemented a prototypical system that facilitates proactive information delivery services using the reinforcement learning technique described. The system has four main components – a visual tool, situation monitor, dispatching and learning module. Fig. 3a shows the overall structure of the system.

We developed a visual tool for specifying situations, information contents and delivery policies. Situation specifications are stored in the situation library in XML formats for the situation monitor to process. Fig. 4 shows a screenshot of the visual tool.

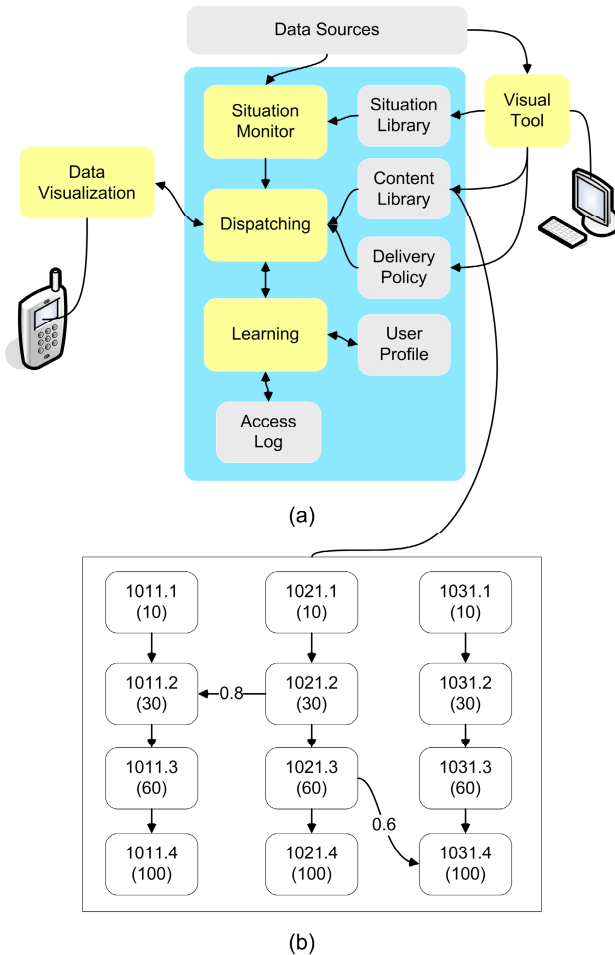


Fig. 3. The overall structure of the proposed proactive information system

The situation monitor consists of a pool of data watchers and a controller. The controller parses the situation specifications and evenly distributes data monitoring tasks to each data watcher. The data watcher periodically checks the values of data elements and sends back the latest status to the controller. The controller keeps track of the status of a situation. Based on the specification, it triggers the information delivery by alerting the dispatching module.

The messages stored in the content library are marked with *message title*, *message type*, *code number*, *level*, *reward value*, *message content*, and *visualization type*. The level of a message indicates a user's level of interest to the message. The content library structures messages in a message hierarchy. Each type of message has several levels of details. At each level, a message can be linked to other types of messages. Whenever the system delivers a message, it attaches two basic options – *cancel delivery* and *get more info*. The *cancel delivery* option notifies the system not to send the same type of message in future deliveries. The *get more info* option requests the system to send more detailed information. If there are links to other types of messages, these links will be delivered as menu options for the user to choose. That is, in addition to the two basic options, a delivered message will be attached with options to get more information on the linked contents.

Each response from users gets a reward value. The reward value is an indicator of interest. It is calculated by the message level. Links to other types of messages get a percentage of the reward value. Fig. 3b shows an example of message hierarchies. Suppose that message 1021.2 is sent. The attached options will be '1) *cancel delivery*', '2) *get more info*', and '3) *more on 1011.2*'. If the user selects 3), the reward value for this type of message will be $30 + 0.8 * 30$, that is, 54. If the user selects 2), the reward value will be the current reward value of 30 plus the reward value at the next level, that is, 90. If the option '1) *cancel delivery*' is selected, the reward value is set to -1, which means that the user is not interested in the delivered message.

Users' responses are traced and stored in the access log. Each record has six attributes – *user id*, *timestamp*, *message id*, *response*, *originating message id* and *location coordinates*. The timestamp and location attributes play an important role in analyzing a user's interaction behaviors with the system. All delivered messages to users have reward values and are stored in the user profile. The reward value is calculated by the following formula:

$$\sum_{t=1}^n (I * Rt)$$

where n is the number of level in content details, I is the percentage value of a link, Rt is the reward value for the level t .

Each message delivery is dictated by a delivery policy. The default delivery policy is delivering messages based on the reward value. The reward value shows which level of message is to be sent. For example, a reward value between 10 and 40 tells the system to deliver the message contents at level 2; a reward value greater than 40 tells the system to deliver the message contents at level 3. We may overwrite the default delivery policy by changing the reward value and level mapping. Location data may also be used to restrict the information delivery. For example, we can specify the system to deliver level 3 contents if the reward value is greater than 65, and we can

also insert other message links in the options. The delivery policy is specified in a XML format. The following text shows an example.

```
<policy id="1011">  
<userid>1238,1233,1452</userid>  
<mapping>  
  <level>1</level>  
  <value>10-35</value>  
</mapping>  
<mapping>  
  <level>2</level>  
  <value>35-60</value>  
  <options>1021.2,1031.2</options>  
</mapping>  
<location>(N49,W122),(N49,W101)</location>  
</policy>
```

The dispatching mechanism is by means of short message services (SMS) and information downloading using a software program written in Sun's J2ME framework. We implemented a visualization program to be used on mobile devices in Adobe Flash. When an SMS message is received, the user selects the link in the message and the visualization program is invoked to download the information from the server. After downloading, it displays an alert to notify the user the arrival of new information. Each delivered message indicates a visualization method. We currently implemented two main visualization methods – textual and graphical. The textual method just displays the message contents in a simple text form. The graphical method shows the message contents in tables and charts. We will illustrate how it works with an example in the next section.

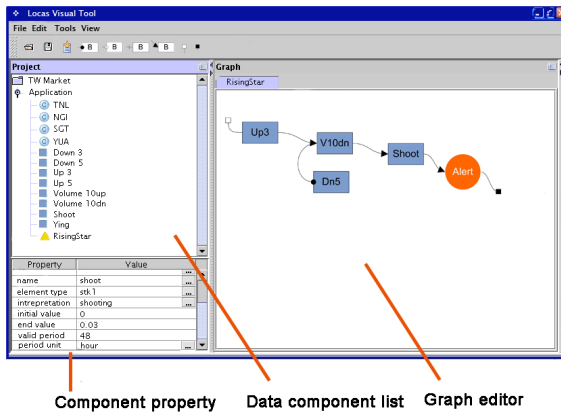


Fig. 4. A screenshot of the visual tool

4.3 An Example

We implemented a stock market alerting system that has the following features:

- a list of alert types with several levels of content details
- users can subscribe to a list of stock alerts
- users have access to the history of sent alerts and responses

On the server side, we developed a data aggregator that collects stock data at an interval of 15 minutes and provides a web service for the situation monitor. We set up a set of situations based on the Japanese candlestick patterns such as shooting star, hanging man, etc. For each stock, we established an entry in the content library which has four levels of details. The data at the highest level contain full information about the stock including its company background, recent and historical financial figures, major shareholders and other related information. Each stock belongs to an industry sector. Stocks of the related sectors have links among them. Each link has a percentage in the degrees of interest. The percentage values are established by calculating the correlation values based on the historical stock data. We analyzed the data for the past two years, and identified the correlated stocks using an association rule technique. We do not discuss the technique here as it is not the focus of this paper.

The communication between users and the system is through SMS messages and data downloads. The user can obtain a list of stock alerts by sending a SMS message to a mobile phone number owned by the system. The server system has a GSM modem attached which picks up all incoming SMS messages. When an alert is triggered by the situation monitor, it checks the subscriber list, and sends out SMS messages to all subscribers based on the corresponding delivery policies.

We set the delivery policy to ensure the user gets same level of contents at least three times before moving up to the next level. That is, they have to select the *get more info* option at each level three times. In terms of the reward value, it has to be added three times to reach the next level. If the same type of an alert is sent 10 times without any reply, the system adjusts the reward value to -1 for that user and gives up future alerts to the same user.

The learning goal for the system is to identify the group of users who are seriously concerned about a set of stocks. These stocks are managed by an investment group who provides investment advice services. Future investment campaigns will first use the list of identified users as the main targeting customers.

During the development of the system, we studied several information visualization methods. As our targeting users are mobile customers, we need a way to fully utilize the limited display space and keep them focused on the presented information. In addition, we wanted to reduce the intrusiveness of an alert as much as possible. The most desirable way is to know what the user is currently doing. There are several methods to achieve this. One way is to obtain the user's daily schedule and current location, and avoid sending alerts while the user is busy, such as in the meeting or possibly driving. The problem for us is that we did not have such data. We resorted to the user access log. We developed a software program that walks through the log and sieves out the time each user most frequently replied to the system. The program establishes a set of time intervals that have higher possibility of getting replies. We added a scheduled delivery feature to the dispatching module which uses the statistics obtained.

Fig. 5 shows a screenshot of the information visualization program on a Nokia mobile phone. A multilevel pie chart is used to give an overview of the interested stocks. The inner circle is formed by the industry sectors, and the outer circle consists of the interested stocks. For each piece in the pie chart, the hue of a color represents the level of increase or decrease. Red color represents an increase, whereas blue color indicates a decrease. The darker the color, the more intense it is. The size of a pie piece shows the trading volume. A detailed candlestick chart is shown by entering the



Fig. 5. Screenshots of mobile data visualization

stock number. The user can request more detailed information in the *options* menu. When the request is sent, the server will register the request and update the user profile as discussed above. Our initial experiments with a group of 50 users were quite positive. We were able to identify a small group of dedicated stock watchers who constantly checked a set of stocks they did not own. More experiments are still needed for more diverse groups of users.

5 Conclusion and Future Work

In this paper, we presented an interval-based approach for specifying situations. We employed a layered model to represent situation-related data. Situations are specified and represented in terms of interval algebra. In order to better understand users' perceptions towards various types of situations, we developed a prototypical proactive system for delivering information to mobile users. We used the reinforcement learning technique to adjust the delivery policy for each user. An example on stock alerts was presented. We showed how our system visualizes mobile data and learns from the user's responses. As it can be seen in our presentation, our approach requires more field studies to improve the learning results. Future work includes investigations into content library structures and content associations. Mobile interactions with the system also require more study.

References

1. Allen, J., Ferguson, G.: Actions and Events in Interval Temporal Logic. *Journal of Logic and Computation* 4(5), 531–579 (1994)
2. Billsus, D., Hilbert, D.M., Maynes-Aminzade, D.: Improving proactive information systems. In: *IUI 2005. Proceedings of the 10th international Conference on intelligent User interfaces*, pp. 159–166 (2005)
3. Budzik, J., Hammond, K., Birnbaum, L.: *Information Access in Context. Knowledge-Based Systems*, vol. 14(1-2). Elsevier Science, Amsterdam (2001)
4. Chittaro, L.: Visualizing Information on Mobile Devices. *Computer* 39(3), 40–45 (2006)

5. Endsley, M.R.: Theoretical underpinnings of situation awareness: A critical review. In: Endsley, M.R., Garland, D.J. (eds.) *Situation Awareness Analysis And Measurement*, LEA, Mahwah, NJ (2000)
6. Greengrass, E.: *Information Retrieval: A Survey* (November 2000), <http://www.csee.umbc.edu/cadip/readings/IR.report.120600.book.pdf>
7. Holz, H., Rostanin, O., Dengel, A., Suzuki, T., Maeda, K., Kanasaki, K.: Task-based process know-how reuse and proactive information delivery in TaskNavigator. In: *CIKM 2006. Proceedings of the 15th ACM international Conference on information and Knowledge Management*, pp. 522–531 (2006)
8. Lieberman, H.: Letizia: An Agent That Assists Web Browsing. In: *Proceedings of the Fourteenth International Joint Conference on Artificial Intelligence*, Montreal, Quebec, Canada, pp. 924–929 (1995)
9. Reiter, R.: *The Situation Calculus Ontology*. *Electronic News Journal on Reasoning about Actions and Change 2* (1998)
10. Yau, S.S., Liu, J.: Incorporating Situation Awareness in Service Specifications. In: *Isorc 2006. Proceedings of the Ninth IEEE international Symposium on Object and Component-Oriented Real-Time Distributed Computing*, vol. 00, pp. 287–294. Washington, DC (2006)

Energy-Efficiency on a Variable-Bitrate Device

Yung-Hen Lee¹, Jian-Jia Chen², and Tei-Wei Kuo²

¹ Advanced Micro Devices (AMD)
henryyh.lee@amd.com

² Department of Computer Science and Information Engineering
National Taiwan University, Taiwan
{r90079, ktw}@csie.ntu.edu.tw

Abstract. Dynamic power management has been adopted in many systems to reduce the power consumption by changing the system state dynamically. This paper explores energy efficiency for systems equipped with PCI Express devices, which are designed for low power consumption and high performance, compared to corresponding PCI devices. We propose dynamic power management mechanism and a management policy for energy-efficient considerations. A case study for a variable-bit-rate LAN device under the PCI Express specification is exploited to provide supports for dynamic packet transmission. Simulation results show that the proposed mechanism and policy would reduce the system energy consumption substantially.

1 Introduction

The designs of high-performance hardware have always been in a strong demand in the past decades. The performance of microprocessors has been improved dramatically, and the improvement process continues for the following foreseeable future. Recently, the needs of energy efficiency in various system components trigger the exploring of the tradeoff between the system performance and the energy consumption. Different techniques in dynamic power management (DPM) [11], dynamic voltage scaling (DVS) [21], and dynamic cache re-sizing are proposed in different contexts and for different applications. DPM aims at the reducing of the power consumption dynamically by changing the system state, and DVS changes the supply voltage of the electronic circuits dynamically for considerations of energy-efficiency.

Energy-efficient real-time scheduling has been an active research topic in the past decade for DVS systems. Researchers have proposed various scheduling algorithms to minimize the energy consumption for periodic hard real-time tasks under different assumptions, e.g., [11, 14]. When fixed-priority scheduling is considered, various energy-efficient scheduling algorithms were proposed based on heuristics [20, 22, 23, 25, 29]. When energy-efficient scheduling of aperiodic real-time tasks is considered, energy-efficient scheduling for uniprocessor environments with a continuous speed spectrum was explored in [8, 28, 3, 27]. Scheduling algorithms were also proposed in the minimization of the energy consumption when there is a finite number of speeds for a processor with negligible speed transition overheads [9, 10, 6, 7, 5].

Under DPM, a device must be in the active state to serve requests, and it might go into the idle or sleep state to save energy. Requests might be issued by applications or

respond to external events, such as the arrival of network packets. Many works on power management mainly focus on the prediction of the duration of each idle period and often assumes that the arrival times of requests cannot be changed [11, 13]. However, the duration of an idle period can be changed by the scheduling (or even delaying) of requests in reality. A common approach is to cluster several short idle periods into a long one such that a device with DPM support could be idle or sleep for a long period of time. There have been some excellent results proposed for processor DPM support, such as those in [12, 19, 26], or for the considerations of real-time task scheduling, such as those in [4, 24]. Existing works mostly consider single service provider or device, e.g., a processor, where how to extend them to the support of multiple devices or a real device is not clear.

This paper explores energy efficiency for systems equipped with Peripheral Component Interconnect (PCI) Express devices, which are designed for low power consumption and high performance, compared to PCI devices [17]. Note that the PCI Express (PCI-E) interface provides control mechanism of functions and parameters for PCI-E devices, such as the supply voltage, the load capacitance, the frequency, and the transfer link [16]. In this work, we propose dynamic power management mechanism for considerations of energy-efficiency. A greedy algorithm for on-line scheduling is proposed to facilitate the power management for a device by re-ordering requests and by reducing the numbers of bitrate changes. We show how to integrate the proposed algorithm and mechanism into existing system implementations. A case study is exploited for a variable-bit-rate local-area-network (LAN) device under the PCI Express specification to provide supports for dynamic packet transmission. The proposed algorithms were evaluated by extensive simulations over networking traces. The experimental results show that the proposed mechanism and policy would reduce the system energy consumption substantially.

The rest of this paper is organized as follows: Section 2 presents the system architecture. Section 3 provides the motivation of this work and define the problem, following the mechanism and the policy in our energy-efficient design for variable-bitrate devices. Section 4 presents the simulation results. Section 5 is the conclusion.

2 System Architecture

2.1 PCI and PCI-Express Specifications

The Peripheral Component Interconnect (PCI) Local Bus is a high-performance 32-bit or 64-bit bus with multiplexed address and data lines. The bus is used for interconnection between highly integrated peripheral controller components, peripheral add-in cards, processors, and memory systems. In the PCI Local Bus Specification, Revision 2.1 [17], states are defined for all PCI functions, i.e., D0, D1, D2, or D3hot. Although, state transition and conditions of power management are defined in the PCI Bus Power Management Interface Specification [15], how to achieve energy efficiency in the hardware (or even software) implementation is unclear in the specification.

PCI defines a device as a physical load on the PCI bus. Each PCI device can host multiple functions, and each device has its own PCI Configuration Space. Since each PCI function is an independent entity to the software, each function must implement its

own power management interface. Each PCI function can be in one of four power management states, i.e., D0, D1, D2, and D3. As defined in the PCI Local Bus Specification, Revision 2.1, all PCI functions must support states D0, D3hot, and D3cold. Power management states provide different levels of power savings, and each state is denoted by a state number. Note that D1 and D2 are optional power management states. These intermediate states are intended to provide system designers more flexibility in balancing power saving, restore time, and performance. For example, the D1 state would consume more energy than the D2 state; however, the D1 state does provide a quicker restore time, compared to the D2 state. The D3 state is belonging to a special category in power management, and a PCI function could be transitted from any state into D3 by a command issued by software code or an action, due to the physical removing of the power from its host PCI device.

The PCI-Express (PCI-E) specification was designed to trade performance for energy consumption. PCI-E adopts control mechanism of functions to do power management. According to the system workload and performance metrics, a PCI-E device might dynamically adjust its supply voltage, transfer link, or frequency to satisfy the system requirements. To apply DPM to a PCI-E device, a power manager (PM) is required in the system to decide the state changes of the device. PM wakes up a device to serve requests and shuts it down to save power. However, any state transition incurs overheads in both energy consumption and latency. Consequently, a device should be shut down only if it can sleep long enough to compensate the performance and energy overhead.

In particular, PM provides the following services [16]:

1. Mechanism to identify power management capabilities of a given function.
2. The ability to turn a function into a certain power management state.
3. Notifications of the current power management state of a function.
4. The option to wake up the system on a specific event.

In addition to the power management of functions, PM also provides Link power management so that the PCI-E physical link could let a device get to an active state, i.e., an initial state, or enable state transition. PCI-E Link states are not visible directly to legacy bus drivers but are derived from the power management states of the components residing on those links. The link states defined in the PCI-E specification are L0, L0s, L1, L2, and L3. The larger the subscript is, the more the power saving. PCI-E components are permitted to wake up the system by using wake-up mechanism, followed by a power management event (PME) message. Even when the main power supply of a device is turned off, a system with the corresponding PCI-E device might be waken up by providing the optional auxiliary power supply (Vaux) needed for the wake-up operation.

2.2 Variable-Bitrate PCI-Express LAN Devices

A system device is, in general, an integration of several application-specific integrated circuits (ASICs). In chip designs, the supply voltage (Vcc) usually supplies voltage to each component or function, as shown in Figure 1(a), where one purpose in the combination of ASICs is to reduce power consumption [18]. ASIC2 and ASIC3 might be merged or redesigned into an integration circuit (IC) because of changes in the design. For example, when several passive units, such as ASIC1 and the rest in Figure 1(a),

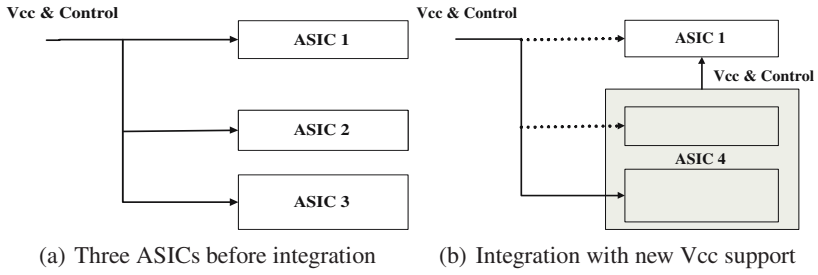


Fig. 1. Low-Power ASICs designs

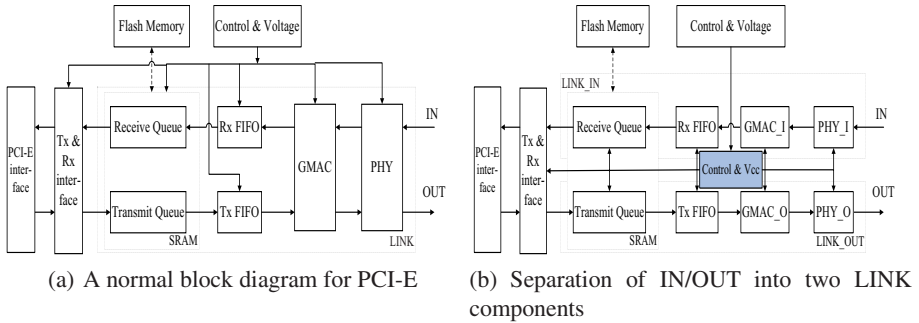


Fig. 2. The block diagram of new LAN devices in which all control and voltage supply belong to the "Control & Vcc" unit

have some dependent relationship or control sequence, the supply voltage circuits can be changed, as shown in Figure 1(b), in which the supply voltage of ASIC1 comes from the integrated IC (ASIC4) of ASIC2 and ASIC3.

This paper revises the existing architecture of LAN card devices based on the PCI-E specification [16]. It should not only manage state transition for power management but also save power. A typical design block diagram of a PCI-E LAN device is shown in Figure 2(a). From right to left in the IN port in Figure 2(a), the components are the physical layer (PHY), the global media access control (GMAC) layer, and the first-in-first-out reception buffer (Rx FIFO). PHY translates the protocol between the signal layer and the physical layer. The GMAC layer translates the protocol between different interfaces. On the other hand, from left to right in Figure 2(a) in the OUT port in Figure 2(a), we have a transmission queue and first-in-first-out transmission buffer (Tx FIFO). Our proposed architecture is shown in Figure 2(b). To reduce the power consumption of the GMAC and PHY layers, we design a control unit to control each function unit or component. Take the LAN card as an example: About a half (IN or OUT transport) of the power consumption is required when only one direction transmission occurs. There are two advantages in this architecture: First, a new control unit for Vcc supply is created, and different voltage supplies could be given to different units based on different needs (if the hardware is properly implemented), e.g., state/frequency

Table 1. Parameters in different LAN bit-rate settings

| LAN Speed (Megabit/Sec) | Transmission Mode | Current (mA) | Power (mW) |
|-------------------------|------------------------------|--------------|------------|
| 1000Mb (1Gb) | Normal Run (Functional Test) | 350.9 | 1157 |
| | Link Up (Idle) | 314.5 | 1137 |
| | Link Down | 139.2 | 459 |
| 100Mb | Normal Run (Functional Test) | 147.7 | 487 |
| | Link Up (Idle) | 131.8 | 434 |
| | Link Down | 120.5 | 398 |
| 10Mb | Normal Run (Functional Test) | 116.4 | 384 |
| | Link Up (Idle) | 95.3 | 314 |
| | Link Down | 87.5 | 298 |

Case 1000 Megabits :

| | | |
|-------------|-------------|--------------|
| (Work):3sec | (Idle):1sec | (Down):46sec |
|-------------|-------------|--------------|

Total energy consumption: $1157 * 3 + 1137 * 1 + 459 * 46 = 25722$ (mJoule)

Case 100 Megabits :

| | | |
|--------------|-------------|--------------|
| (Work):30sec | (Idle):1sec | (Down):19sec |
|--------------|-------------|--------------|

Total energy consumption: $487 * 30 + 434 * 1 + 398 * 19 = 22606$ (mJoule)

Case Variable-Bitrate :

| | | | | | |
|---------------|------------|---------------|--------------|--------------|---------------|
| 100Mb(W):1sec | 1G(W):3sec | 100Mb(W):1sec | 10Mb(W):1sec | 10Mb(I):1sec | 10Mb(D):43sec |
|---------------|------------|---------------|--------------|--------------|---------------|

Total energy consumption: $487 * 1 + 1157 * 3 + 487 * 1 + 384 * 1 + 314 * 1 + 298 * 43 + 860 * 2 + 322 * 1 = 19999$ (mJoule)

Fig. 3. An example in the transmissions of 300 MB of data in 50 seconds by a PCI-E LAN device

changes. Secondly, the new architecture separates IN and OUT into two functions, such as LINK_IN and LINK_OUT in Figure 2(b).

The power consumption of the proposed variable bit-rate device (VBD) LAN device is summarized in Table 1. When the bit-rate of the device changes from 1000Mb (1Gb) to 100Mb, the state transition will take about 860 mJ. When the bit-rate of the device changes from 100Mb to 10Mb, state transition will take about 322 mJ. The state transition overhead between different D states could be considered negligible, since it takes less than 10 mW power consumption with negligible timing overhead.

3 An Energy-Efficient Design for Variable-Bitrate PCI-E Devices

This section shows an energy-efficient design for variable-bitrate devices. we first describe the problem definition and provide an example. Secondly, we propose mechanism for state transition on the variable-bitrate device. Thirdly, we design a policy to make variable-bitrate device work properly.

3.1 Problem Definition

Suppose that we are required to transmit 300Mb of data from a host computer via a PCI-E LAN device to another computer in 50 seconds. Let the actual data transmission rate in the networking environment be 0.1 times of the network transmission bit-rate.

There are several alternatives in executing the data transmission: We might choose to transmit data in 1Gb, as shown in the first item in Figure 3. Three seconds are used to transmit data, and one second is used to have state transition of the device to the idle state. The rest of 46 seconds is for the device to stay at the "Down" state. Another alternative is to transmit data at 100Mb for 30 seconds and then let the device go into the idle state. The device would stay at the "Down" state for the rest 20 seconds, as shown in the second item in Figure 3. The other alternative is intelligently exploit the flexibility in the switching of bit-rates. For example, we could do bit-rate adjustments, as shown in the third item in Figure 3. In terms of the energy consumption, the third alternative is the best among the presented alternatives, and the first is the worst. The third could save more than 20% of the total energy consumption, compared to the first. More than 10% saving of the total energy consumption could be achieved by the third alternative, compared to the second case. Note that it is not feasible to transmit the data at 10Mb because we could not finish it in 50 seconds. The example shows the advantage of adaptive adjustments of transmission bit-rates in energy consumption and provides a motivation for our work. Note that it is infeasible to have an optimal schedule unless the future is predictable.

This paper explores the management of state transition and transmission-bit-rate adjustments for the scheduling of requests. Each request to the device under considerations is characterized by three parameters: its Input/Output type, start-time, and request size. Our objective is to minimize the energy consumption in servicing the requests such that the task response time is acceptable. In the following subsections, we shall propose state transition mechanism based on existing system implementations and the PCI-E specification. We will then propose a policy in the management of state transition and transmission-bit-rate adjustments with the considerations of the scheduling of requests.

3.2 A Time-Slice-Based Transition Algorithm: The Basic Approach

The main data structure in the variable-bitrate driver is a queue. When a new request arrives, the request is inserted into the queue with the specification of its own transmission direction, starting time, and request size. This queue will be processed by applying the shortest-job-first (SJF) order for better performance since it tends to minimize the average response time of requests. Each request is associated with a status variable to record its service status. A request is removed from the queue after its service is completed.

We exploit the idea of *time slice* for the servicing of requests to a variable bit-rate device. The operating time of a device is divided into fixed time slices (of a specified length T) such that both the bit-rate and the power management state of the device are required to remain unchanged within each time slice. The rationale behind the time-slice idea is to reduce the number of bit-rate switchings to save energy consumption when requests are interleaved with short inter-arrival time. Another incentive is to keep the device working when some request finishes before the expiration of the time slice so that any immediately incoming request within the time-slice period would be serviced instantly.

Let D_c and F_c be the device state and the bit-rate state of the device, respectively. F_b denotes the actual bit-rate in the previous time slice. Initially, let $D_c = D_0$, $F_c = 100\text{Mb}$, and $F_b = 1\text{Mb}$, regardless of what the network transmission bit-rate is. At the starting

Algorithm 1. A Time-Slice-Based Transition Algorithm

Input: (F_c, D_c, F_b) **Output:** The setting of the state D_c and the bit-rate F_c for this time slice, where F_b is the bit-rate for the previous time slice**if** the device is not working **then****if** $F_c > F_{min}$ **then**Downgrade F_c with one degree**else****if** $D_c > D_{min}$ **then**Downgrade D_c with one degree**else****if** (F_c can be upgraded with one degree and $F_c < F_{max}$) **then**Upgrade F_c with one degree**else****if** the actual bit-rate in the previous time slice is less than F_b **then**Downgrade F_c with one degree**else** F_c remains F_b is set as the actual bit-rate in the previous time slice;

of each time slice, F_c and D_c are set as the actual device transmission bit-rate and the device state in the previous time slice, respectively, and $F_b = F_c$. The device transmission bit-rate (referred to as the bit-rate) and the state is checked up, as shown in Algorithm 1. F_c could be one of the three bit-rates 10Mb, 100Mb, and 1000Mb. D_c could be one of the three states: D0 (working state), D1 (idle state), and D3 (link down state, also abbreviated as D_{min}). Given a variable bit-rate LAN device, let the minimum transmission bit-rate F_{min} and the maximum transmission bit-rate F_{max} be 10Mb and 1Gb, respectively.

We adopt a greedy algorithm to set up the bit-rate and the state of a device at the starting of each time slice. The basic idea is as follows: If the device is not working, and the current transmission bit-rate F_c is higher than the minimum bit-rate F_{min} , then we downgrade the bit-rate. If the current device state D_c is higher than the minimum device state D_{min} , then we turn the device into a deeper power saving state. On the contrary, if the device is working (in default, the device will recover to the D0 state), and the bit-rate could be upgraded, then we shall pull the device bit-rate to a higher level for the performance considerations. If the actual bit-rate in the previous time slice is less than F_b , then the upgrading of the bit-rate would not improve the performance. As a result, we downgrade F_c with one degree. When we downgrade (upgrade) F_c with one degree, we mean that we move down (up) the bit-rate to the next level of the available bit-rate settings. Similarly, when we downgrade (upgrade) D_c with one degree, we mean that we move down (up) the state to the next level of the available D-state settings.

3.3 A Revised Algorithm

The purpose of this subsection is to further improve the time-slice-based transition algorithm with the considerations of the bit-rate of the three time slices ahead of the current

| | | |
|---|---|---|
| Set bit-rate : DR_3 Actual bit-rate : AR_3 | Set bit-rate : DR_2 Actual bit-rate : AR_2 | Set bit-rate : DR_1 Actual bit-rate : AR_1 |
|---|---|---|

t (current time)

Fig. 4. The notations of the bit-rates of the time slices ahead of the current time slice

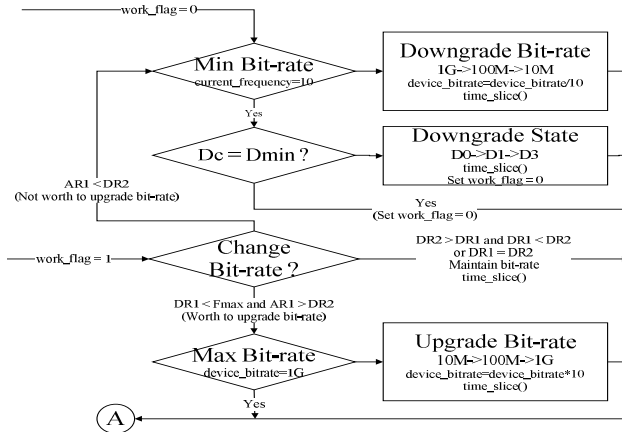
time slice: The revised version of the algorithm is referred to as the *variable bit-rate algorithm*. Let t denote the starting time of the current time slice. We shall determine the device state D_c and the bit-rate state F_c of the device. Let DR_x and AR_x denote the set bit-rate and the actual bit-rate of the device in the x -th time slice ahead of the current time slice, respectively, as shown in Figure 4. Note that even if we set the bit-rate of a device at a value, the actual bit-rate might be lower because the device and the environment might not allow such as a bit-rate. The variable bit-rate algorithm is a greedy algorithm based on the idea of the time-slice-based transition algorithm.

The rules in the upgrading and downgrading of the bit-rate for the variable bit-rate algorithm is defined as follows:

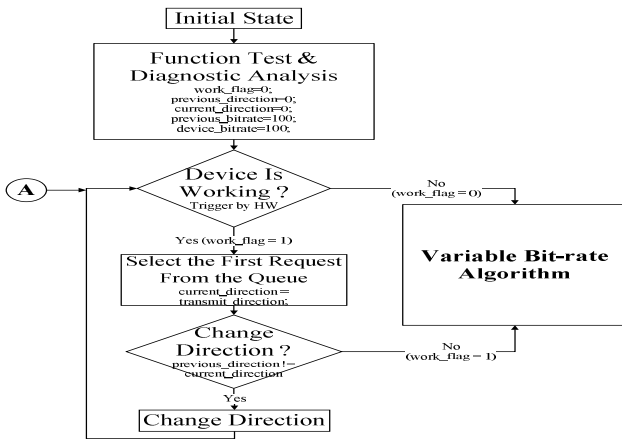
1. Downgrade the transmission bit-rate F_c if any of the following two conditions is satisfied:
 - The device is not working, and $DR_1 >$ minimum transmission bit-rate.
 - The device is working, and $AR_1 < DR_2$.
2. Downgrade the device state D_c if both of the following two conditions are satisfied:
 - The device is operating at the minimum transmission bit-rate.
 - The current state is over the minimum device state.
3. Upgrade the transmission bit-rate F_c if the following condition is satisfied:
 - The device is working, DR_1 is lower than the maximum device bit-rate, and $AR_1 > DR_2$.
4. Upgrade the device state D_c if the following condition is satisfied:
 - The device is not working, but a new request arrives.
5. The state and the bit-rate of the device remain as the same as their corresponding ones in the previous time slice if any of the following two conditions is satisfied:
 - The device is working, $DR_2 > DR_3$, and $DR_1 < DR_2$.
 - The device is working, and $DR_2 = DR_1$.

The flowchart of the rules is illustrated in Figure 5(a), where $work_flag = 0$ means that the device is not working; otherwise, it is working.

The operating of the device is shown in Figure 5(b). The device starts at the initial state and does various function test and diagnostic analysis. Flags $work_flag$, $previous_direction$, $current_direction$, $previous_bitrate$, and $device_bitrate$ denote the working status (i.e., working or not working), the status of the previous time slice (i.e., read or write), the status of the current time slice (i.e., read or write), the set bit-rate of the previous time slice, and the set bit-rate of the current time slice, respectively. If the device is not working, then call the variable-bit algorithm; otherwise, the request at the front of the queue is selected for data transmission. $current_direction$ is set as the transmission direction of the request, i.e., read or write. If the direction is not changed, then invoke the variable-bit algorithm; otherwise, the transmission direction is changed by a hardware setting action. Note that circuits for "IN" and "OUT" are



(a)



(b)

Fig. 5. The flowchart of the variable bit-rate algorithm

separated, as shown in Figure 2(b). The hardware setting action would activate a different circuit and de-activate the original circuit for the service of the previous request. The selected request will be executed by the newly activated circuit. The entire operating of the device will go back to the checking state of the device working status.

The variable bit-rate algorithm provides a framework for the adjustment of the state and the bit-rate of a device. The algorithm could be further improved by considering the tradeoff between the power consumption and the required bit rate. Take Table 1 as an example. The first column of the table shows the three available bit-rates of a variable-bit-rate LAN device, and the second column shows the three available states for each bit-rate, e.g., the *Normal Run* state being as *D0* of the bit-rate 1000Mb. The third column and the fourth column show the current and the power of each corresponding state for a given bit-rate. We should further improve the conditions in the upgrading and downgrading of states/bit-rates by considering the tradeoff between the energy

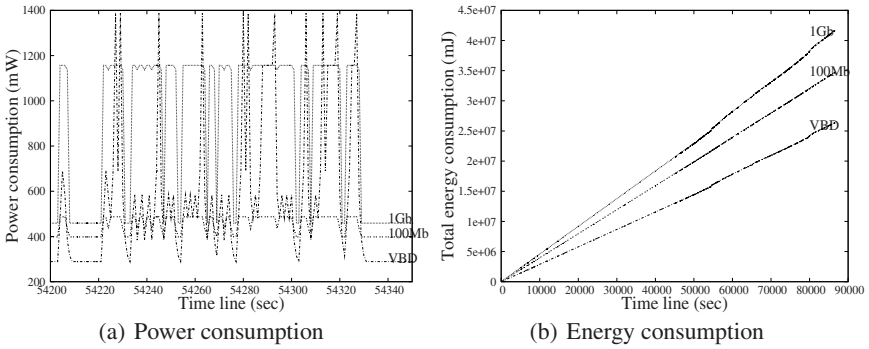


Fig. 6. Power consumption and energy consumption in different bit-rate settings

consumption and the bit-rate, i.e., the performance. For example, since the power ratio between 1Gb and 100Mb at the *Normal Run* state is 2.376, there is no point to move to 1Gb from 100Mb if the transmission bit-rate required for a transmission does not need to be 2.376 times faster. Another consideration is on the limitation on the actual transmission bit-rate in the reality. When a device could not reach the transmission bit-rate as being set by the algorithm, the maximum transmission bit-rate should be set accordingly. Such a setting action could be done dynamically as the policy requires, e.g., once per few hours.

4 Performance Evaluation

The proposed algorithm was evaluated over a trace collected at an FTP server for two weeks. The arrival times of transmission requests were translated into their start times in the trace. The range of time slices varied from one second to five seconds. The power consumption values of a bit-rate transition, a D state transition, and data transmissions are as shown in Section 2. Three different strategies were simulated: Setting of the transmission bit-rate fixed at 1Gb but with possible state transitions (denoted to as 1Gb), Setting of the transmission bit-rate fixed at 100Mb but with possible with state transition (denoted to as 100Mb), and our proposed variable-bit-rate algorithm (denoted to as VBD).

Figure 6(a) shows the power consumption under the 1Gb strategy, the 100Mb strategy, and the VBD strategy with a one-second time slice. As astute readers might point out, the 1Gb strategy always had a larger power consumption for most of the time, compared to other strategies. With the VBD strategy, the power consumption was usually smaller, but there did exist some peaks in the experiments because of switchings of the bit-rate. (Note that the power consumption in the switching of states was negligible.) Figure 6(b) shows the total energy consumption of the three strategies under comparisons. The VBD strategy clearly outperformed the other two strategies. The relationship between the energy consumption and the time line was almost linear for each of the three strategies although they had different slopes. The gap between the VBD

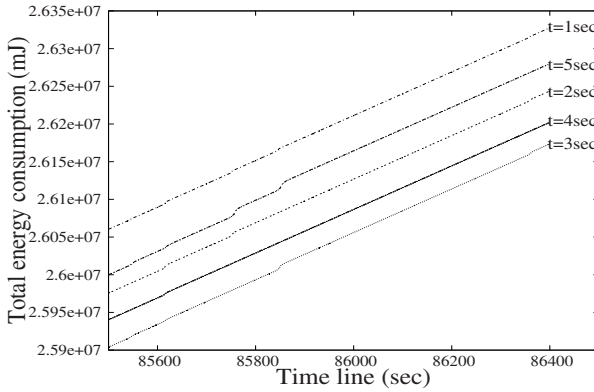


Fig. 7. The energy consumption of the VBD strategy in different settings of time slices

Table 2. The average response time in different durations of a time slice

| Time slice (second) | N/A(1Gb) | 1 second | 2 second | 3 second | 4 second | 5 second |
|-----------------------------|----------|----------|----------|----------|----------|----------|
| Average Response Time (sec) | 0.206 | 0.646 | 0.653 | 0.658 | 0.664 | 0.679 |

strategy and others was getting bigger as time went by. By the end of the experiments, the VBD strategy could save roughly 30% of the energy consumption, compared to the 1Gb strategy. Compared to the 100Mb strategy, the VBD strategy could save roughly 15% of the energy consumption.

Figure 7 shows the experimental results of the VBD strategy by varying the duration of a time slice from one second to five seconds. In the experiments, the VBD strategy with three-second time slice is better than that with others. The difference between any two of the total energy consumption of the five lines was, in fact, less than 1%. The determination of time-slice durations in the experiments was done by a series of experiments and observations. We found that the durations adopted in the experiments were the best for the trace under simulation. However, we must point out that a bad decision for a time-slice duration would not ruin the proposed VBD strategy too much. It was based on the observation in which the performance of the VBD strategy did not change a lot for the five durations. Even if the duration was set as infinity, the VBD strategy became the 1Gb strategy. The determination of time slice could be determined by profiling tools.

In general, the VBD strategy paid the price at a worse response time, compared to the 1Gb strategy. The average response time of the VBD strategy with different durations of a time slice and the 1Gb strategy are shown in Table 2. Although the average response time of the VBD strategy was worse than that of the 1Gb strategy, the delay in the transmission of a file was not bad because the delay was only for the transmission of the last piece of the file (when a file was broken into pieces for transmissions).

5 Conclusion and Future Work

In this paper, we design a prototype of a variable-bit-rate local-area-networking device over the PCI Express specification. A case study is done over a variable-bit-rate local-area-networking (LAN) device under the PCI Express specification in energy-efficient designs. A greedy on-line scheduling algorithm is developed to minimize the energy consumption with tolerable performance degradation. We propose the concept of time slice to adjust the transmission bit-rate or the idle time of the device. A feasible mechanism is presented based on the implementations of existing systems. The proposed algorithm and mechanism were evaluated by simulations over emulated devices. The experimental results show that the proposed algorithm could reduce from 15% to 30% energy consumption roughly, compared to a typical PCI-E LAN card with normal PM functionality. The increasing of the average response time of requests was reasonable in the experiments.

Energy efficiency has been a highly critical design issue in hardware and software designs. For the future work, we shall further extend the static time-slice approach to a dynamic one to further improve the power saving of the system. The concept and methodology proposed in this work could also be extended to the energy-efficient management designs of complicated devices, such as many VGA, USB, ATAPI and SATA devices. Such management designs could be implemented by either software or hardware, and there is always a tradeoff in terms of cost and performance.

References

1. Aydin, H., Melhem, R., Mossé, D., Mejía-Alvarez, P.: Determining optimal processor speeds for periodic real-time tasks with different power characteristics. In: Proceedings of the IEEE EuroMicro Conference on Real-Time Systems, pp. 225–232 (2001)
2. Aydin, H., Melhem, R., Mossé, D., Mejía-Alvarez, P.: Dynamic and aggressive scheduling techniques for power-aware real-time systems. In: Proceedings of the 22nd IEEE Real-Time Systems Symposium, pp. 95–105 (2001)
3. Bansal, N., Kimbrel, T., Pruhs, K.: Dynamic speed scaling to manage energy and temperature. In: Proceedings of the Symposium on Foundations of Computer Science, pp. 520–529 (2004)
4. Brown, J.J., Chen, D.Z., Greenwood, G.W., Hu, X., Taylor, R.W.: Scheduling for power reduction in a real-time system. In: International Symposium on Low Power Electronics and Design, pp. 84–87 (1997)
5. Chen, J.-J., Kuo, T.-W.: Procrastination for leakage-aware rate-monotonic scheduling on a dynamic voltage scaling processor. In: LCTES. ACM SIGPLAN/SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems, pp. 153–162 (2006)
6. Chen, J.-J., Kuo, T.-W., Lu, H.-I.: Power-saving scheduling for weakly dynamic voltage scaling devices. In: Dehne, F., López-Ortiz, A., Sack, J.-R. (eds.) WADS 2005. LNCS, vol. 3608, pp. 338–349. Springer, Heidelberg (2005)
7. Chen, J.-J., Kuo, T.-W., Shih, C.-S.: $1+\epsilon$ approximation clock rate assignment for periodic real-time tasks on a voltage-scaling processor. In: EMSOFT. The 2nd ACM Conference on Embedded Software, pp. 247–250 (2005)
8. Irani, S., Shukla, S., Gupta, R.: Algorithms for power savings. In: Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms. Society for Industrial and Applied Mathematics, pp. 37–46 (2003)

9. Ishihara, T., Yasuura, H.: Voltage scheduling problems for dynamically variable voltage processors. In: Proceedings of the International Symposium on Low Power Electronics and Design, pp. 197–202 (1998)
10. Kwon, W.-C., Kim, T.: Optimal voltage allocation techniques for dynamically variable voltage processors. In: Proceedings of the 40th Design Automation Conference, pp. 125–130 (2003)
11. Benini, L., Bogliolo, A., Micheli, G.D.: A survey of design techniques for system-level dynamic power management. *IEEE Transactions on VLSI Systems* (2000)
12. Lorch, J.R., Smith, A.J.: Scheduling techniques for reducing processor energy use in macos. *Wireless Networks*, 311–324 (1997)
13. Lu, Y.-H., Chung, E.-Y., Simunic, T., Benini, L., Micheli, G.D.: Quantitative comparison of power management algorithms. *Design Automation and Test in Europe* (2000)
14. Mejía-Alvarez, P., Levner, E., Mossé, D.: Adaptive scheduling server for power-aware real-time tasks. *ACM Transactions on Embedded Computing Systems* 3(2), 284–306 (2004)
15. PCI Bus Power Management Interface Specification 1.1 (December 1998)
16. PCI Express Base Specification 1.0a (April 2003)
17. PCI Local Bus Specification 2.3 (March 2002)
18. Putting it All Together: Intel's Wireless-Internet-on-a-Chip (June 2001)
19. Qu, G., Potkonjak, M.: Power minimization using system-level partitioning of applications with quality of service requirements. In: ICCAD, pp. 343–346 (1999)
20. Quan, G., Hu, X.: Minimum energy fixed-priority scheduling for variable voltage processor. In: Proceedings of the Design Automation and Test Europe Conference, pp. 782–787 (2002)
21. Rabaey, J.M., Chandrakasan, A., Nikolic, B.: *Digital Integrated Circuits*, 2nd edn. Prentice-Hall, Englewood Cliffs (2002)
22. Shin, D., Kim, J., Lee, S.: Low-energy intra-task voltage scheduling using static timing analysis. In: Proceedings of the 38th Conference on Design Automation, pp. 438–443. ACM Press, New York (2001)
23. Shin, Y., Choi, K.: Power conscious fixed priority scheduling for hard real-time systems. In: Proceedings of the 36th ACM/IEEE Conference on Design Automation Conference, pp. 134–139. ACM Press, New York (1999)
24. Shin, Y., Choi, K.: Power conscious fixed priority scheduling for hard real-time systems. In: DAC, pp. 134–139 (1999)
25. Shin, Y., Choi, K., Sakurai, T.: Power optimization of real-time embedded systems on variable speed processors. In: Proceedings of the 2000 IEEE/ACM International Conference on Computer-Aided Design, pp. 365–368. IEEE Press, Los Alamitos (2000)
26. Weiser, M., Welch, B., Demers, A., Shenker, S.: Scheduling for reduced cpu energy. In: Symposium on Operating Systems Design and Implementation, pp. 13–23 (1994)
27. Yang, C.-Y., Chen, J.-J., Kuo, T.-W.: Preemption control for energy-efficient task scheduling in systems with a DVS processor and Non-DVS devices. In: RTCSA. The 13th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (2007)
28. Yao, F., Demers, A., Shenker, S.: A scheduling model for reduced CPU energy. In: Proceedings of the 36th Annual Symposium on Foundations of Computer Science, pp. 374–382. IEEE, Los Alamitos (1995)
29. Yun, H.-S., Kim, J.: On energy-optimal voltage scheduling for fixed-priority hard real-time systems. *ACM Transactions on Embedded Computing Systems* 2(3), 393–430 (2003)

The Secure DAES Design for Embedded System Application

Ming-Haw Jing¹, Jian-Hong Chen¹, Zih-Heng Chen¹, and Yaotsu Chang^{1,2}

¹ Department of Information Engineering, I-Shou University,
Ta-Hsu, Kaohsiung 84001, Taiwan
mhjing@isu.edu.tw, d9503001@stmail.isu.edu.tw,
d9403001@stmail.isu.edu.tw

² Department of Applied Mathematics, I-Shou University,
Ta-Hsu, Kaohsiung 84001, Taiwan
ytchang@isu.edu.tw

Abstract. Recently, Advanced Encryption Standard (AES) has become one of the major symmetric encryption algorithms used in the embedded system applications. Many researches extended use of the algorithm of AES for system security. In this paper, we propose a diversified AES (DAES) to create more variations. In the architecture of the DAES, the diversity results from the modification of the parameters of DAES. In the process of system design, the additional parameters may not only cause operational complexity but also influence the security. In this article, a method to measure the security of DAES is also provided. We propose a strategy to optimize the design of the DAES with higher security from the scope of S-box via repeating property and MixColumn polynomials via branch number. During the analysis procedure, the size of embedded program may also be reduced.

Keywords: Advanced Encryption Standard, branch number, data security, embedded system, repeating property, symmetric encryption algorithms.

1 Introduction

In regard to the security of the communication in embedded systems, Advanced Encryption Standard (AES) is the major symmetric encryption algorithm. In 2002, Barkan and Biham proposed a list of a total of 240 dual ciphers of AES which can be used to resist the side channel attacks [1]. Side channel attacks are effective only when a cracker knows the encryption algorithm. Because the dual cipher of AES increases variety in encryption, it raises the level of difficulty in cracking the key. Concerning the measurement of the security of symmetric cryptography, the delay time used to compute the key and S-box in AES is the major factor since the speed of system computation has been continuously improved. In the near future, the safety of AES will face the same tough challenge which can be found in the current circumstances in DES. For this reason, we proposed an extended AES with more variations, which is called Diversified AES (DAES) [2].

The architecture of DAES is based on the original AES, and the changes of parameters of DAES provide variations. DAES is able to provide higher security against the side channel attacks, and it even has the characteristics of defending unknown attacks in the future. As a result of many combinations of the parameters in DAES, there exist so many ways of implementations of DAES in software. Through the different parameters, DAES are in a huge variety, and these parameters are helpful for the key management in various data security applications. In the embedded system, the software optimization and security must be considered, especially in the applications of relatively large data processing to power-efficient sensors in embedded systems. The first important key factor of security of DAES is the SubBytes with the characteristic of its non-linear transformation. We discovered that the defect of S-box of AES can refer to the repeating property [3]. Another key factor of security is the branch number in the MixColumn operation. The branch number is in direct proportion to the confusion level in the MixColumn operation. According to the above two views of security of DAES, we proposed a method to determine the superior parameters with higher security.

The organization of this article is as follows: The mathematical background of this article and DAES architecture are described in Sect. 2. The properties of S-box and MixColumn polynomials are presented in Sect. 3. The analyses and statistical chart of security of DAES are discussed in Sect. 4. Finally, the brief conclusions are made in Sect. 5.

2 Preliminaries

We know that the cryptanalysis has many ways to attack cryptographic system in key management [4]. The human factors included cause even more problems. For example, the systems have been working for a long period or frequently running in real time with reduced complexity (such as using a simple hashing function to replace the non-linear part). The main reason is that these attacks focus on the keys. Therefore, the most serious problem is key loss due to weak protocol or internal break-in (like betrayer). As a result, the demand for a new cryptographic system rises, in order to prevent from causing an immediate risk of key loss. To meet this demand, extra parameter(s) should be added to the system other than the key without increasing system complexity. The DAES system actually has 4 parameters used in each round: (1) field irreducible polynomial; (2) the substitution through S-box of the SubBytes; (3) the shift in the ShiftRows; and (4) the polynomial $a(x)$ of the MixColumns. The main key and parameters can be negotiated by different channels between the encryption and decryption sides. This will increase the difficulty in gaining access to the information for attackers. Reference [2] also initiated the idea of using dual ciphers to create a Rijndael-like system. Next, the variations of these parameters will be introduced in particular using different irreducible polynomials.

We know that the computation in $GF(2^8)$ is formed by taking polynomials over $GF(2)$ modulo an irreducible polynomial $f(x)$. The multipliers and multiplicative inverse operations in $GF(2^8)$ are affected by the irreducible polynomial. In AES,

| | | | |
|-----------|-----------|-----------|-----------|
| $a_{0,0}$ | $a_{0,1}$ | $a_{0,2}$ | $a_{0,3}$ |
| $a_{1,0}$ | $a_{1,1}$ | $a_{1,2}$ | $a_{1,3}$ |
| $a_{2,0}$ | $a_{2,1}$ | $a_{2,2}$ | $a_{2,3}$ |
| $a_{3,0}$ | $a_{3,1}$ | $a_{3,2}$ | $a_{3,3}$ |

Fig. 1. The state

Rijndael uses the irreducible polynomial $f(x)=x^8+x^4+x^3+x+1$ to be a modular polynomial in $GF(2^8)$. According to Rijndael's description: The polynomial $f(x)$ ('11B') for the multiplication in $GF(2^8)$ is the first one in the list of irreducible polynomials of degree 8; the reason to choose this irreducible polynomial is that it's the first polynomial of the degree 8 listed in [5]. In fact, there exist 30 irreducible polynomials with degree 8 over $GF(2)$. Each of them can serve as the irreducible polynomial to be used in a DAES system. With the cipher key, various irreducible polynomials may be regarded as an extra input or key of the DAES system and be helpful in the key management. In addition, two major factors which influence the security of DAES refer to the variations of S-box in the SubBytes, and polynomials in the MixColumns.

2.1 The S-Box of SubBytes

In the SubBytes, the S-box applied on the input x is mapped to its multiplicative inverse x^{-1} , where $x \in GF(2^8)$. The multiplicative inverse varies according to the different field polynomials. In DAES, the S-box is given by Eq. (1)

$$x' = Lx^{-1} + c, \quad x^{-1} = L^{-1}(x' + c), \quad (1)$$

in encryption and decryption, respectively, where L is one of the invertible 8×8 matrices over $GF(2)$, L^{-1} is the inverse matrix of L , and c is a non-zero constant. According to Eq. (1), the various irreducible polynomial $f(x)$ produces different S-box in SubBytes of DAES.

2.2 The MixColumn Polynomial

In MixColumn operation of the DAES system, they can be characterized by a pair of four-term polynomials $c(x)$ and $d(x)$ which are the inverses of each other when are modulo $x^4 + 1$, called the MixColumn and InvMixColumn polynomials, respectively. The operations of the AES algorithm are performed on a 4×4 array of bytes called the State and denoted by A , as shown in Fig. 1.

In the encryption process, the function of the MixColumn can be realized by the following steps: First, associate the first column of the State A with a four-term polynomial over $GF(2^8)$; the first column of A gives $a_{0,0}x^3 + a_{1,0}x^2 + a_{2,0}x + a_{3,0}$. Secondly,

Table 1. Four Pairs of Invertible Polynomials

| $c(x)$ | $d(x)$ |
|--|--|
| $\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ | $\{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$ |
| $\{01\}x^3 + \{01\}x^2 + \{02\}x + \{03\}$ | $\{0e\}x^3 + \{0b\}x^2 + \{0d\}x + \{09\}$ |
| $\{01\}x^3 + \{02\}x^2 + \{03\}x + \{01\}$ | $\{09\}x^3 + \{0e\}x^2 + \{0b\}x + \{0d\}$ |
| $\{02\}x^3 + \{03\}x^2 + \{01\}x + \{01\}$ | $\{0d\}x^3 + \{09\}x^2 + \{0e\}x + \{0b\}$ |

multiply the obtained polynomial by the MixColumn polynomial $c(x)$ which is given by

$$c(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}. \tag{2}$$

Next, divide the product by the modulus polynomial $x^4 + 1$ to get a four-term polynomial. Finally, associate the resulting four-term polynomial with a vector and then replace the original first column of state a by this vector. Running the same procedures for every other column of the State matrix A gives a complete run of the MixColumn transformation. On the other hand, the procedures in the InvMixColumn transformation are almost the same as those in the MixColumn transformation. The only difference is that the resulting polynomial obtained from the first step is multiplied by $d(x)$ instead of by $c(x)$ in the second step, where $d(x)$ is used in the inverse polynomial of $c(x)$ and is given by

$$d(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}. \tag{3}$$

In the following, a number of pairs of $(c(x), d(x))$ are proposed as examples to replace the default pair of transformations in MixColumn and InvMixColumn, as shown in Table 1.

3 The Properties of Security

3.1 The Cyclic Groups in S-Box

In this section, we focus on the repeating property of non-linear layer, SubBytes transformation of DAES. We know each byte in the information block is byte wise substituted by the SubByte using S-box. The influence of each SubByte can be regarded as a function. Combined functions can be denoted by $f^n(I) = f \circ f \circ \dots \circ f(I)$, where I is the input value in the block. The period (the number of repetition) of $f(I)$ is defined by $f^{period}(I) = I$.

In AES, every input byte of S-box returns to the initial value after t period of the substitution [3]; i.e., for any i of the S-box $= f(i)$, $f^t(i) = i$. The 256 values of the input bytes can be classified into five small sets as in Table 2 according to the period t . The period of each set is 87, 81, 59, 27 and 2, respectively. Besides, the authors in [3] took the LCM (least common multiple) into consideration to calculate the maximal period. The maximal period is in direct proportion to the security of S-box. In this case, the LCM is 277182.

Table 2. Classifying the substitution in the S-box of AES

| | | | | | | | | | | | | | | | | | | | |
|--------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Set 1 (t=87) | | | | | | | | | | | | | | | | | | | |
| F2 | 89 | A7 | 5C | 4A | D6 | F6 | 42 | 2C | 71 | A3 | 0A | 67 | 85 | 97 | 88 | C4 | 1C | 9C | DE |
| 1D | A4 | 49 | 3B | E2 | 98 | 46 | 5A | BE | AE | E4 | 69 | F9 | 99 | EE | 28 | 34 | 18 | AD | 95 |
| 2A | E5 | D9 | 35 | 96 | 90 | 60 | D0 | 70 | 51 | D1 | 3E | B2 | 37 | 9A | B8 | 6C | 50 | 53 | ED |
| 55 | FC | B0 | E7 | 94 | 22 | 93 | DC | 86 | 44 | 1B | AF | 79 | B6 | 4E | 2F | 15 | 59 | CB | 1F |
| C0 | BA | F4 | BF | 08 | 30 | 04 | | | | | | | | | | | | | |
| Set 2 (t=81) | | | | | | | | | | | | | | | | | | | |
| 7C | 10 | CA | 74 | 92 | 4F | 84 | 5F | CF | 8A | 7E | F3 | 0D | D7 | 0E | AB | 62 | AA | AC | 91 |
| 81 | 0C | FE | BB | EA | 87 | 17 | F0 | 8C | 64 | 43 | 1A | A2 | 3A | 80 | CD | BD | 7A | DA | 57 |
| 5B | 39 | 12 | C9 | DD | C1 | 78 | BC | 65 | 4D | E3 | 11 | 82 | 13 | 7D | FF | 16 | 47 | A0 | E0 |
| E1 | F8 | 41 | 83 | EC | CE | 8B | 3D | 27 | CC | 4B | B3 | 6D | 3C | EB | E9 | 1E | 72 | 40 | 09 |
| 01 | | | | | | | | | | | | | | | | | | | |
| Set 3 (t=59) | | | | | | | | | | | | | | | | | | | |
| 00 | 63 | FB | 0F | 76 | 38 | 07 | C5 | A6 | 24 | 36 | 05 | 6B | 7F | D2 | B5 | D5 | 03 | 7B | 21 |
| FD | 54 | 20 | B7 | A9 | D3 | 66 | 33 | C3 | 2E | 31 | C7 | C6 | B4 | 8D | 5D | 4C | 29 | A5 | 06 |
| 6F | A8 | C2 | 25 | 3F | 75 | 9D | 5E | 58 | 6A | 02 | 77 | F5 | E6 | 8E | 19 | D4 | 48 | 52 | |
| Set 4 (t=27) | | | | | | | | | | | | | | | | | | | |
| EF | DF | 9E | 0B | 2B | F1 | A1 | 32 | 23 | 26 | F7 | 68 | 45 | 6E | 9F | DB | B9 | 56 | B1 | C8 |
| E8 | 9B | 14 | FA | 2D | D8 | 61 | | | | | | | | | | | | | |
| Set 5 (t=2) | | | | | | | | | | | | | | | | | | | |
| 73 | 8F | | | | | | | | | | | | | | | | | | |

In DAES, we try to change the parameters in S-box, but it may influence the maximal period in S-box. For example, we replace the nonzero constant 0x63 with the 0xE3. The components in this S-box are classified into 11 sets, of which the period is {103,63,44,27,7,3,3,2,2,1,1}. In this case, there are two elements whose period is one. Although the LCM in this case is 856548, which is more than that in AES (277182), this makes S-box have lower security. For this case, the elements whose period is one are 0x1C and 0x51; i.e., $f(0x1C) = 0x1C$ and $f(0x51) = 0x51$. Therefore, we can't evaluate the security by LCM. We provide a method to measure the security of DAES comparing with the AES using Eq. (4).

$$R_x = \frac{P_{\max}(DAES)}{P_{\max}(AES)}$$

$$P_{\max}(DAES) = \begin{cases} 0 & , \text{if there exists a element which period is 1} \\ \text{the L.C.M of the set} & , \text{others} \end{cases} \quad (4)$$

$$P_{\max}(AES) = 277182.$$

According to the Eq. (4), the R_x of the DAES whose nonzero constant changes to 0xE3 is 0. There are many varieties of DAES, whose R_x is higher than that of AES. For instance, we replace the nonzero constant with 0x67. The set becomes {76,72,43,36,13,10,6} and $P_{\max}(DAES)=3823560$, $R_x=1379.44\%$. The elements of each set are listed in Table 3.

Table 3. List elements of sets when nonzero constant is changed to 0x67

| | | | | | | | | | | | | | | | | | | | |
|--------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Set 1 (t=76) | | | | | | | | | | | | | | | | | | | |
| 78 | B8 | 68 | 41 | 87 | 13 | 79 | B2 | 33 | C7 | C2 | 21 | F9 | 9D | 5A | BA | F0 | 88 | C0 | BE |
| AA | A8 | C6 | B0 | E3 | 15 | 5D | 48 | 56 | B5 | D1 | 3A | 84 | 5B | 3D | 23 | 22 | 97 | 8C | 60 |
| D4 | 4C | 2D | DC | 82 | 17 | F4 | BB | EE | 2C | 75 | 99 | EA | 83 | E8 | 9F | DF | 9A | BC | 61 |
| EB | ED | 51 | D5 | 07 | C1 | 7C | 14 | FE | BF | 0C | FA | 29 | A1 | 36 | 01 | | | | |
| Set 2 (t=72) | | | | | | | | | | | | | | | | | | | |
| 73 | 8B | 39 | 16 | 43 | 1E | 76 | 3C | EF | DB | BD | 7E | F7 | 6C | 54 | 24 | 32 | 27 | C8 | EC |
| CA | 70 | 55 | F8 | 45 | 6A | 06 | 68 | 7B | 25 | 3B | E6 | 8A | 7A | DE | 19 | D0 | 74 | 96 | 94 |
| 26 | F3 | 09 | 05 | 6F | AC | 95 | 2E | 35 | 92 | 4B | B7 | AD | 91 | 85 | 93 | DB | 65 | 49 | 3F |
| 71 | A7 | 58 | 6E | 9B | 10 | CE | 8F | 77 | F1 | A5 | 02 | | | | | | | | |
| Set 3 (t=43) | | | | | | | | | | | | | | | | | | | |
| F6 | 46 | 5E | 5C | 4E | 2B | F5 | E2 | 9C | DA | 53 | E9 | 1A | A6 | 20 | B3 | 69 | FD | 50 | 57 |
| 5F | CB | 1B | AB | 66 | 37 | 9E | 0F | 72 | 44 | 1F | C4 | 18 | A9 | D7 | 0A | 63 | FF | 12 | CD |
| B9 | 52 | 04 | | | | | | | | | | | | | | | | | |
| Set 4 (t=36) | | | | | | | | | | | | | | | | | | | |
| 2F | 11 | 86 | 40 | 0D | D3 | 62 | AE | E0 | E5 | DD | C5 | A2 | 3E | B6 | 4A | D2 | B1 | CC | 4F |
| 80 | C9 | D9 | 31 | C3 | 2A | E1 | FC | B4 | 89 | A3 | 0E | AF | 7D | FB | 0B | | | | |
| Set 5 (t=13) | | | | | | | | | | | | | | | | | | | |
| 7F | D6 | F2 | 8D | 59 | CF | 8E | 1D | A0 | E4 | 6D | 38 | 03 | | | | | | | |
| Set 6 (t=10) | | | | | | | | | | | | | | | | | | | |
| 67 | 81 | 08 | 34 | 1C | 98 | 42 | 28 | 30 | 00 | | | | | | | | | | |
| Set 7 (t=6) | | | | | | | | | | | | | | | | | | | |
| A4 | 4D | E7 | 90 | 64 | 47 | | | | | | | | | | | | | | |

3.2 Branch Number in MixColumn

Daemen and Rijmen [6] proposed a definition of branch number to evaluate the security of MixColumn for the suitable choice of the coefficients. In this section, we also use this idea to evaluate the security of all the MixColumn polynomials of DAES. We first give a brief review of the branch number [6]. Let F be a linear transformation acting on byte vectors and let the byte weight $W(a)$ of state a be the total number of nonzero bytes in state a . The diffusion power of a linear transformation can be quantified and measured by the following definition:

Definition 1. The branch number of a linear transformation F is

$$\min_{a \neq 0} (W(a) + W(F(a))). \tag{5}$$

Here, a nonzero byte in the state a is called an active byte. A state consists of four columns. Each column has four entries. In a byte-weight-one state, there is only one nonzero entry among the 16 entries; i.e., there is only one nonzero column whose byte weight is one. For MixColumn, there are 4 active bytes in the output of state a , as MixColumn acts on the columns independently. Hence, the upper bound for the branch number is 5. If the branch number is 5, a difference in 1 input (or output) byte propagates to all 4 output (or input) bytes, a 2-byte input (or output) difference to at least 3 output (or input) bytes. Therefore, the sum of byte weights of the two states, before MixColumn operation and after MixColumn operation, is 5 at least.

Table 4. The three pairs of invertible polynomials

| $c(x)$ | $d(x)$ |
|--|--|
| $\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ | $\{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$ |
| $\{01\}x^3 + \{01\}x^2 + \{02\}x + \{03\}$ | $\{0e\}x^3 + \{0b\}x^2 + \{0d\}x + \{09\}$ |
| $\{01\}x^3 + \{02\}x^2 + \{03\}x + \{01\}$ | $\{09\}x^3 + \{0e\}x^2 + \{0b\}x + \{0d\}$ |
| $\{02\}x^3 + \{03\}x^2 + \{01\}x + \{01\}$ | $\{0d\}x^3 + \{09\}x^2 + \{0e\}x + \{0b\}$ |

Table 5. The four examples of type 1 polynomials

| $b(x)$ |
|--|
| $\{01\}x^3 + \{02\}x^2 + \{01\}x + \{03\}$ |
| $\{05\}x^3 + \{0e\}x^2 + \{05\}x + \{0f\}$ |
| $\{09\}x^3 + \{0a\}x^2 + \{09\}x + \{0b\}$ |
| $\{0c\}x^3 + \{04\}x^2 + \{0c\}x + \{05\}$ |

In DAES, the branch number of $c(x)$ of MixColumn may be considered necessary. From our analysis, there exist many parameters with branch number being 5. Next, we propose a solution to find the polynomial used in MixColumn with branch number 5.

3.2.1 Property of MixColumn Polynomials

There are three properties of the MixColumn and InvMixColumn polynomials, and these properties will be useful in the security of implementation of the DAES in embedded software. First, each pair of invertible polynomials $c(x)$ and $d(x)$ mentioned above can be used to produce three more pairs of four-term invertible polynomials. Before we state Property 1, we give a new notation: If c, d are vectors, let $c_{(k)}$ be the k -fold left-cyclic-shift of c and $d_{(-k)}$ be the k -fold right-cyclic-shift of d .

Properties 1. $d_{(-1)}(x) = c_{(1)}^{-1}(x)$, $d_{(-2)}(x) = c_{(2)}^{-1}(x)$, and $d_{(-3)}(x) = c_{(3)}^{-1}(x)$.

The three pairs of invertible polynomials promised by the Property 1 are shown in Table 4.

Next, in some special cases, the MixColumn and InvMixColumn polynomials are the same. Property 2 serves as a sufficient condition for this kind of polynomial.

Properties 2. Let $c(x)$ be a four-term polynomial. If $c_1 = c_3$, and $c_0 + c_2 = \{01\}$, then $c^{-1}(x) = c(x)$. Polynomials that satisfy this property are called Type 1 polynomial. Table 5 shows four examples of type 1 polynomials.

Combining the above two properties, one can easily observe the following property.

Table 6. The four examples of type 2 polynomials

| $c(x)$ |
|--|
| $\{02\}x^3 + \{01\}x^2 + \{03\}x + \{01\}$ |
| $\{0e\}x^3 + \{05\}x^2 + \{0f\}x + \{05\}$ |
| $\{0a\}x^3 + \{09\}x^2 + \{0b\}x + \{09\}$ |
| $\{04\}x^3 + \{0c\}x^2 + \{05\}x + \{0c\}$ |

Table 7. The type 3 polynomials generator table 1

| | |
|--|--|
| $\{01\}x^3 + \{02\}x, \{0e\}x^3 + \{0d\}x$ | $\{01\}x^2 + \{03\}, \{0b\}x^2 + \{09\}$ |
| $\{02\}x^3 + \{01\}x, \{0d\}x^3 + \{0e\}x$ | $\{03\}x^2 + \{01\}, \{09\}x^2 + \{0b\}$ |
| $\{04\}x^3 + \{07\}x, \{0b\}x^3 + \{08\}x$ | $\{04\}x^2 + \{06\}, \{0e\}x^2 + \{0c\}$ |
| $\{05\}x^3 + \{06\}x, \{0a\}x^3 + \{09\}x$ | $\{05\}x^2 + \{07\}, \{0f\}x^2 + \{0d\}$ |
| $\{06\}x^3 + \{05\}x, \{09\}x^3 + \{0a\}x$ | $\{06\}x^2 + \{04\}, \{0c\}x^2 + \{0e\}$ |
| $\{07\}x^3 + \{04\}x, \{08\}x^3 + \{0b\}x$ | $\{07\}x^2 + \{05\}, \{0d\}x^2 + \{0f\}$ |

Table 8. The type 3 polynomials generator table 2

| | |
|--|--|
| $\{01\}x^3 + \{03\}x, \{09\}x^3 + \{0b\}x$ | $\{01\}x^2 + \{02\}, \{0d\}x^2 + \{0e\}$ |
| $\{03\}x^3 + \{01\}x, \{0b\}x^3 + \{09\}x$ | $\{02\}x^2 + \{01\}, \{0e\}x^2 + \{0d\}$ |
| $\{04\}x^3 + \{06\}x, \{0c\}x^3 + \{0e\}x$ | $\{04\}x^2 + \{07\}, \{08\}x^2 + \{0b\}$ |
| $\{05\}x^3 + \{07\}x, \{0d\}x^3 + \{0f\}x$ | $\{05\}x^2 + \{06\}, \{09\}x^2 + \{0a\}$ |
| $\{06\}x^3 + \{04\}x, \{0e\}x^3 + \{0c\}x$ | $\{06\}x^2 + \{05\}, \{0a\}x^2 + \{09\}$ |
| $\{07\}x^3 + \{05\}x, \{0f\}x^3 + \{0d\}x$ | $\{07\}x^2 + \{04\}, \{0b\}x^2 + \{08\}$ |

Properties 3. Let $c(x) = (c_3, c_2, c_1, c_0)$ be a four-term polynomial. If $c_0 = c_2$, and $c_1 + c_3 = \{01\}$, then $c^{-1}(x) = (c_1, c_2, c_3, c_0)$. Polynomials of this kind are called Type 2 polynomial.

For example, if $c(x) = \{02\}x^3 + \{01\}x^2 + \{03\}x + \{01\}$, we can get $d(x) = \{03\}x^3 + \{01\}x^2 + \{02\}x + \{01\}$. Table 6 shows four examples of type 2 polynomials that belong to this class.

Besides the Type 1 and 2 polynomials explained above, the rest of the four-term polynomials are categorized into Type 3. After an exhausting search, we found that all the Type 3 polynomial pairs can be produced by the following steps: Pick up any pair of polynomials from the six pairs of polynomials in the left column of Table 7 (resp. Table 8), and then add these two polynomials to any pair of polynomials from the six pairs of polynomials in the right column of Table 7 (resp. Table 8). The two polynomials obtained will be a Type 3 polynomial pair.

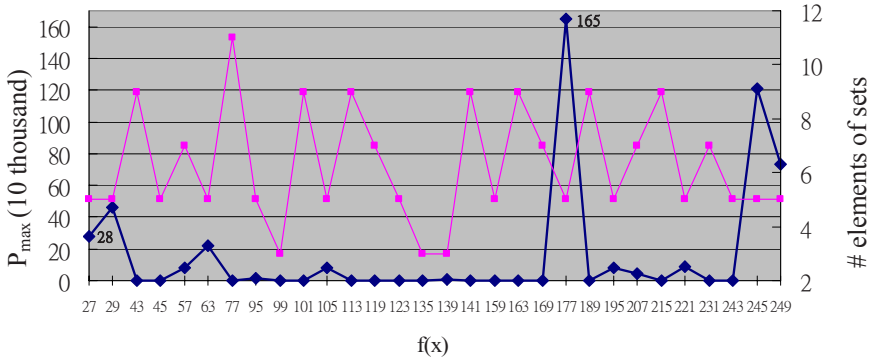


Fig. 2. The statistic for Pmax v.s. F(x)

For example, taking row 3 from the left column of Table 7 and row 1 in the right column, two polynomial pairs will be obtained, namely, ({04}x³+{01}x²+{07}x+{03} , {0b}x³+{0b}x²+{08}x+{09}) and ({04}x³+{01}x²+{07}x+{03} , {0b}x³+{0b}x²+{08}x+{09}). Obviously, both of them are Type 3 polynomial pairs.

4 System Analysis

4.1 Statistic of S-Box in DAES

The secure measurement is considerable in the S-box because the S-box is the only non-linear layer transformation in DAES algorithm. We have mentioned in Eq. (4) of the use of the LCM to measure the maximum period that is called P_{max}. It is in direct proportion to the security of S-box. We gather the data of S-box with different f(x) via simulation software and draw the line chart as Fig. 2. The x coordinate axis is f(x) with decimal representation. The left Y coordinate axis is the P_{max}, whose unit is ten thousand. The right Y coordinate axis is the count of each small group. We have made the following inference:

1. The P_{max} is 1,648,200 while f(x) is x⁸+x⁷+x⁵+x⁴+1=0 ; the representation in decimal without x⁸ is 177. It is about 5.95 times more than AES, whose P_{max} is 277,182 with the f(x) is x⁸+x⁴+x³+x¹+1=0 ; the representation in decimal is 27.
2. There exist 16 items whose P_{max} is 0; that is to say, the f(x) has a great influence on P_{max}.
3. The count of small sets is not in direct proportion to the P_{max}.

4.2 Branch Number of MixColumns in DAES

Therefore, after applying the MixColumn, the output of a byte-weight-one state has a byte weight of at most 4 because the MixColumn acts on the columns independently.

Hence, the upper bound for the branch number is 5. Therefore, the sum of byte weights of the two States, before MixColumn operation and after MixColumn operation, is at least 5. It is obvious that {00} is invalid. After an exhausting calculation, the branch number of all the Type 3 polynomials mentioned in Section 3 is at least 5. However, in the case of Type 1 and Type 2 polynomials, a byte-weight-two input may produce a byte-weight-two output whose branch number equals 4.

In system design, the complexity of embedded software design using Type 3 polynomials may be reduced, and the security of such software is better than that of the software using Type 1 and Type 2. As a result, type 3 polynomial is considered and analyzed.

5 Conclusions

In this article, we present a way of measurement to design the S-box and MixColumns in DAES, which is related to the embedded data security application. We have proposed approaches to find the specific parameters with better abilities to defend various attacks in the DAES systems. The abilities regarding S-box or MixColumns include the maximum period P_{\max} and branch number, respectively. As a result, choosing $f(x) = x^8 + x^7 + x^5 + x^4 + 1$ as the module polynomial and MixColumns polynomials in type 3 has better code efficiency with higher security in DAES.

Acknowledgements. This work is supported in part by the Nation Science Council, Taiwan, under grant NSC 96-2623-7-214-001-D.

References

1. Barkan, E., Biham, E.: In How Many Ways Can You Write Rijndael? In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 160–175. Springer, Heidelberg (2002)
2. Jing, M.H., Chen, Z.H., Chen, J.H., Chen, Y.H.: Reconfigurable System for High-Speed and Diversified AES using FPGA. *Microprocessors & Microsystems* 31, 94–102 (2007)
3. Song, B., Seberry, J.: Further Observations on the Structure of the AES Algorithm. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 223–234. Springer, Heidelberg (2003)
4. Dobbertin, H., Knudsen, L., Robshaw, M.: The Cryptanalysis of the AES - a Brief Survey. In: Dobbertin, H., Rijmen, V., Sowa, A. (eds.) *Advanced Encryption Standard – AES*. LNCS, vol. 3373, pp. 1–10. Springer, Heidelberg (2005)
5. Lidl, R., Niederreiter, H.: *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge (1986)
6. Daemen, J., Rijmen, V.: *The Rijndael Block Cipher* (1999)

Software Power Peak Reduction on Smart Card Systems Based on Iterative Compiling

Matthias Grumer¹, Manuel Wendt¹, Stefan Lickl¹ Christian Steger¹,
Reinhold Weiss¹, Ulrich Neffe², and Andreas Mühlberger²

¹ Institute for Technical Informatics
Graz University of Technology
{grumer,wendt,steiger,rweiss}@iti.tugraz.at
² NXP Semiconductors
Business Line Identification
{ulrich.neffe, andreas.muehlberger}@nxp.com

Abstract. RF-powered smart cards are widely used in different application areas today. The complexity and functionality of smart cards is growing continuously. This results in a higher power consumption. The power consumed is heavily depending on the software executed on the system. The power profile, especially the power peaks, of an executed application influence the system stability. If the power consumed by such a device exceeds the power provided by the RF-field a reset can be triggered by the power control unit or otherwise the chip may stay in an unpredictable state. Flattening the power profile can thus increase the stability of a system.

We present an optimization system which intends to eliminate critical peaks after the analysis of the power profile of an executed application. In an iterative compile process an optimal tradeoff between power and performance has to be found. This is achieved by selecting or deselecting different optimization passes on the intermediate language level of the compiler.

Keywords: Iterative compiling - Software power optimization - Peak reduction - Smart card systems - Power profile analysis.

1 Introduction

The complexity and functionality of smart cards is growing continuously. This results in a higher power consumption of such devices. Smart cards are often supplied by a radio frequency (RF) field which provides a strictly limited amount of power. If the power consumed by such a device exceeds this limit, a reset can be triggered by the power control unit or otherwise the chip may stay in an unpredictable state [1]. Furthermore the transmission from RF-system to a reader is often done via amplitude shift keying. Power peaks, which result in an unwanted modulation of the field, can potentially disturb the communication. Therefore the smart card has to be optimized for low power with the constraint to avoid peaks in power consumption. Smart cards are often used to process

and store confidential information. Simple power analysis (SPA) and differential power analysis (DPA) are attacks based on the analysis of the power consumption profile of a smart card [2]. Eliminating power peaks and thus flattening the power consumption profile can hinder these attacks.

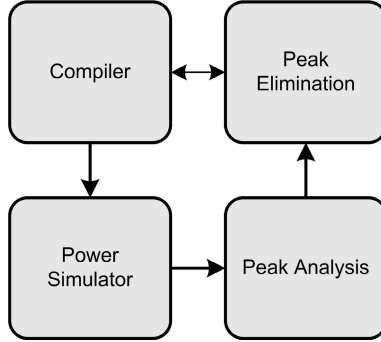


Fig. 1. Peak elimination framework - Overview

To address these problems different solutions to reduce the power consumption at different system levels have been proposed. As power peaks are mainly caused by determined instruction sequences, in this work we focus on the software level. We present a new concept, where the optimization is done in an iterative compile process. As depicted in Fig. 1 the source code is first compiled and then executed on a cycle accurate *power simulator*. The simulator delivers a cycle accurate power profile of the executed code. The *peak analysis unit* is able to identify critical peaks from the power profile and informs the *peak elimination unit* of the corresponding code segments. The *compiler* tries to eliminate these critical power peaks by selecting or deselecting the different compiler passes for these code segments. This whole cycle is repeated in an iterative manner to find the optimal trade-off between performance and system stability.

The remainder of this paper is organized as follows. Section 2 surveys related work for software power optimization and iterative compiling. In section 3 the classification of peaks is described. Section 4 depicts the peak elimination framework. Results are presented in section 5. The conclusions are summarized in section 6.

2 Related Work

Tiwari et al. [3,4] outlined the importance of energy optimization at the software level in embedded systems already in the nineties. They presented different optimization techniques for reducing the software energy consumption, such as the use of a code-generator-generator and reordering the instructions. All these techniques are based on instruction level power analysis. The underlying energy

model defines base costs (BC) to characterize a single instruction. The circuit state overhead (CSO) describes circuit switching activity between two consecutive instructions.

On a higher level of compilation a promising technique for the reduction of power peaks is iterative compiling. Iterative Compiling was first presented by Knijnenburg et al. [5,6]. They propose to generate many variants of source programs and to select the best one by profiling these variants. The main problem is to find the best solution in the extremely large search space. They propose to randomly evaluate a small percentage of the transformation space. Fursin et al. [7] demonstrated hill-climbing and random iterative search techniques to optimize large applications on a loop-level.

Cooper et al. [8,9,10] and later Kulkarni et al. [11] demonstrated that finding optimal optimization order can also considerably improve code quality and performance.

Fursin and Cohen [12] presented an Interactive Compilation Interface (ICI). The main goals are to control only the decision process at global and local levels and to avoid revealing all intermediate compiler representations to allow further transparent compiler evolution and to treat current optimization heuristic as a black-box and progressively adapt it to a given program and given architecture. The interface supports different search strategies like exhaustive search, random search, hill-climbing search and machine learning. Although the interface should also support tuning programs for best power consumption, the authors have not shown this in any experiments.

While performance optimization is the main objective in research about iterative compiling, Gheorghita et al. use iterative compilation to reduce energy consumption [13]. The authors use iterative compilation in order to find the best compiled code for energy and energy-delay product. However the work only concentrates on the loop transformation passes.

In this work we propose to use iterative compiling for the power peak reduction on all compiler passes influencing the power behavior of an application.

3 Peak Classification

Figure 2 (a) depicts a peak, which is critical for the system. The peak causes the voltage to drop under the threshold, under which the proper functionality of the processor can not anymore be guaranteed. In the depicted example this threshold is 1.6 V. Whether a peak is critical for the system depends on the shape of the peak himself and on the energy storage capacitor of the system.

Furthermore not only single peaks are critical for the system, but also sequences of peaks. Figure 2 (b) shows a sequence of two peaks. While neither the first peak nor the second one would be critical for the system if appearing alone, the sequence of the two is critical because the supply voltage has not enough time to recover.

Peaks can also be classified according to their origin. Peaks can be produced from both, hardware and software. Software-peaks arise from the execution of

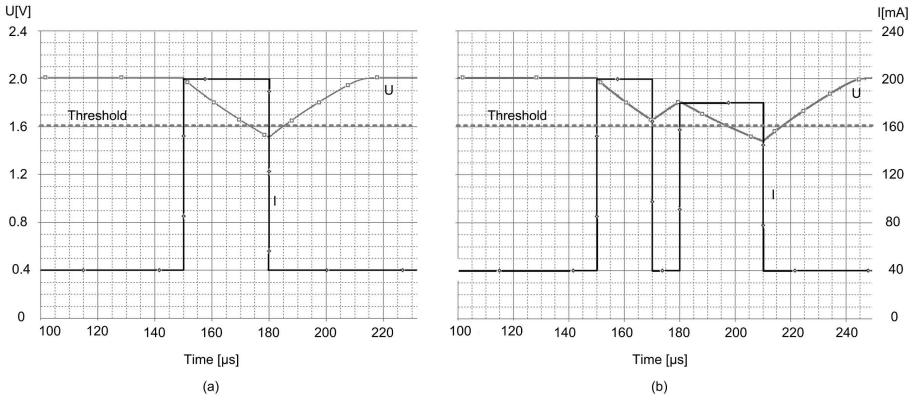


Fig. 2. Critical peaks for system stability: (a) single peak; (b) sequence of peaks

power intensive code segments. Hardware-peaks result for example from the usage of peripherals. Furthermore critical peaks can also arise from a combination of hardware and software-peaks.

Table 1. Classes of peaks and counter measurements

| | Single peak | Sequence of peaks |
|------------------------|--|---|
| Software-peak | - Compiler optimization - Insertion of nonfunctional code | - Compiler optimization - Insertion of nonfunctional code |
| Hardware-peak | - No elimination possible | - Scheduling of peripheral activity |
| Software/Hardware-peak | | - Scheduling of peripheral activity - Compiler optimization - Insertion of nonfunctional code |

Table 1 summarizes the different classes of peaks and depicts possible counter measurements. Single or sequences of software-peaks may be eliminated by the insertion of nonfunctional code. Nonfunctional Code should always be selected in such a way, that circuit state overhead costs are minimized, e.g. an $ADD A, 0$ should be selected if the last instruction executed was an ADD . In the case of single peaks, this lowers the power level over the time and hinders the production of a critical peaks. In the case of sequences of peaks, the nonfunctional code in between two software peaks enables the recovery of the energy storage capacitor. Single hardware-peaks can not be eliminated from the software engineer’s point of view. Sequences of hardware-peaks can be avoided by scheduling the peripheral activizy in such a manner that there is enough time for the energy storage capacitor to recover. The hardware/software-peaks allow a combination of the presented counter measurements. On software level the compiler optimization is also a good strategy to prevent critical peaks. This work concentrates on this

optimization and presents a corresponding framework in the next section. In a later step the framework will also support the other methods presented for peak elimination.

4 Peak Elimination Framework

The whole framework is depicted in Fig. 3. The source code of an application is compiled to target code. As *compiler* the GNU Compiler Collection (GCC) is used. The target architecture is a MIPS32 4KSc processor. The target code is then executed via a debugger on an cycle accurate *instruction set power simulator*, which delivers the power profile of the executed code. A *peak analysis unit* detects all critical peaks and generates a peak report. The *peak elimination unit* decides based on the peak report the level of optimization for each function of the application.

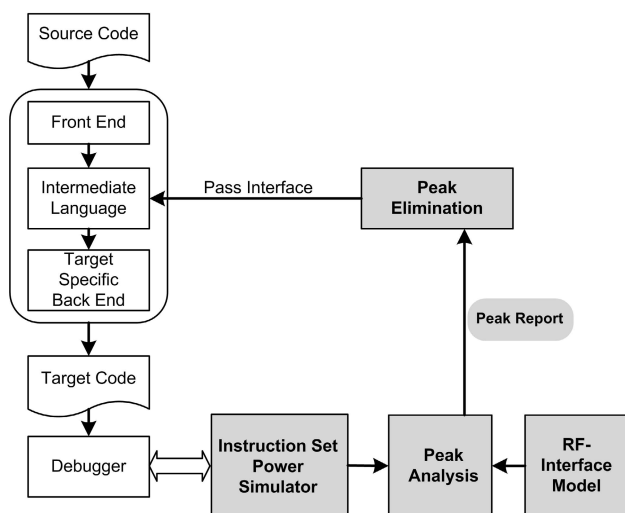


Fig. 3. Peak elimination framework

The following sections describe first the power analysis of different compiler passes and then the peak elimination framework in more detail.

4.1 Power Analysis

First the impact on the power consumption of the different optimization passes of the compiler has been analyzed. For this purpose different benchmarks with different optimization levels have been compiled by deselecting passes with the corresponding compiler flags. The resulting executables have been simulated on the power simulator.

Table 2 depicts the results for some passes of the benchmark *bubblesort*. The bold values are always referenced to the not optimized code (O0). The other values are referenced to the corresponding O-level, e.g. level O1 without the flag *-tree-ch* executes 19.5% slower then level O1 with *-tree-ch*.

Table 2. Analysis of *bubblesort*

| Pass | Gain [%] | | | |
|---------------------------|---------------|---------------|---------------|-------------|
| | Cycles | Energy | Std-dev | Mean Power |
| cse-skip-blocks | -77.59 | -76.81 | -23.65 | 3.46 |
| delayed-branch | -4.11 | -3.80 | 1.78 | 0.32 |
| gcse | -79.58 | -78.93 | -23.35 | 3.21 |
| no-delayed-branch | -75.51 | -75.13 | -15.20 | 1.57 |
| O1 | -79.54 | -78.90 | -23.32 | 3.15 |
| O1 no-loop-optimize | 0.37 | 0.33 | 0.15 | -0.04 |
| O1 no-tree-copy-rename | 19.11 | 17.87 | 7.69 | -1.04 |
| O1 no-tree-ch | 19.50 | 19.41 | 4.56 | -0.07 |
| O1 no-tree-dominator-opts | 9.56 | 8.18 | -0.74 | -1.26 |
| O1 schedule-insn | -0.19 | -0.09 | -0.22 | 0.09 |
| O1 schedule-insn2 | -0.19 | -0.09 | -0.52 | 0.10 |
| O2 | -79.58 | -78.14 | -22.80 | 7.06 |
| O2 no-gcse | 0.00 | 0.00 | -0.02 | 0.00 |
| O2 no-cse-skip-blocks | -0.01 | -3.57 | -1.17 | -3.56 |
| O2 no-schedule-insns2 | 0.00 | 0.00 | 0.31 | 0.00 |
| Os | -75.59 | -74.00 | -15.60 | 6.53 |

The results show clearly, that the total energy consumed is heavily depending on the execution time. Thus optimizations of the performance usually also influence the total energy consumption in a positive way. While the total energy consumption decreases, the mean power typically increases. It can be deduced, that the power level is higher and thus resulting peaks are more critical for the system. This fact is also depicted in Fig. 4. It clearly shows, that the power level increases with the level of optimization.

The lower standard deviation is possibly caused by the higher mean power and not from peak reduction. Results of other benchmarks show that a certain pass can influence the power and energy consumption in different manners, depending on the application. That is why it is not possible to make an optimal pass selection a priori.

Therefore we propose the following strategy: a peak detection system identifies critical parts of the code. The compiler then tries to modify these parts of the code. This can be achieved by selecting or deselecting different compiler passes on a basic block or function level in an iterative process. The resulting code is a trade-off between performance and system stability.

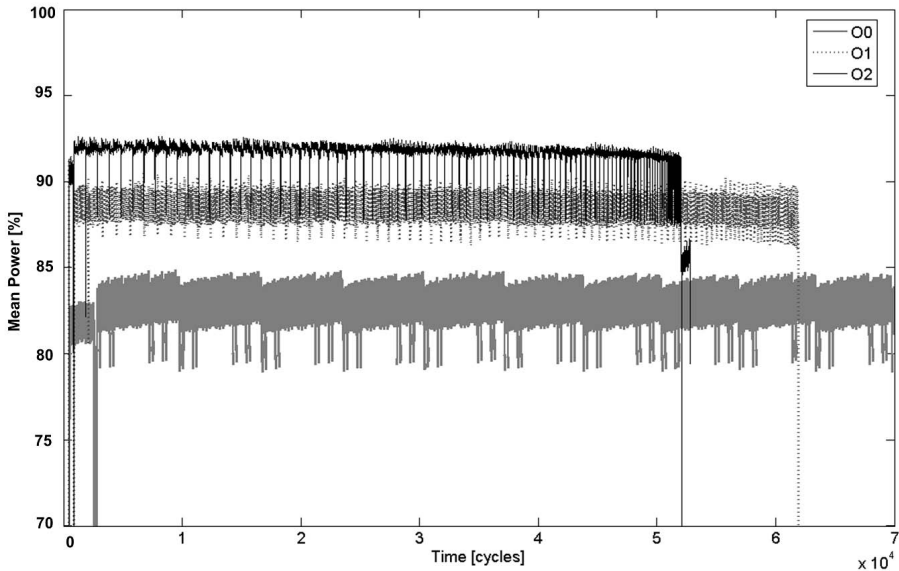


Fig. 4. Power profile segment of *bubblesort* with different optimization levels

4.2 Peak Elimination

Following the proposed strategy we have implemented a peak elimination framework. A preliminary compile cycle is necessary to get a first power profile. The power profile is produced from an instruction set simulator, which was enhanced by an energy model. The energy model developed is a flexible and accurate combination of an instruction-level energy model and a data dependent model based on Tiwari et al. [3] and was presented in [14]. The first compilation is done with the highest optimization level. The peak analysis unit delivers all code segments which produce a critical peak. At the moment we use the mean power windowed over a certain amount of cycles for this purpose. In a next step a model of the RF-interface, which can calculate the voltage level from a given current profile, will be integrated. As the pass manager of GCC works on a function level, in a first approach the framework works on this level as well.

The peak elimination unit deselects the highest pass of the compilation for all functions with critical peaks. An interface to the GCC pass manager, which allows an easy selection of passes, has been implemented for this purpose. We use an external file to communicate with the compiler. The file has an entry for each function of the application with the corresponding optimization level. During the compilation process, the pass manager reads from this file the passes to execute for every function. After each compile cycle the resulting power profile is analyzed again and compared to the previous profile. If the peak size has increased, the deselected pass is selected again. Otherwise, if the peak has decreased but is still too high, the next pass is deselected. The main steps of the algorithm are the

following. **MaxPower** stands for the maximum of the windowed mean power of each function:

1. *Compile with highest optimization level.*
2. *(While the **MaxPower** of any function > threshold) and (the lowest optimization level is not reached):*
 - (a) *For all function with **MaxPower** > threshold:*
 - i. *Deselect highest pass.*
 - (b) *Recompile application.*
 - (c) *If the new **MaxPower** > the old **MaxPower**:*
 - i. *Select pass again.*

This whole loop is repeated either until there is no peak left or there is no pass remaining to be deselected. In the last case, the system reports that there are still critical peaks in the code, which can not be eliminated from the framework.

5 Experimental Results

For first experiments we have defined a threshold for the mean value over each segment of a defined amount of cycles of the power profile. The values for threshold and amount of cycles allow easily to define critical peaks, which have to be eliminated.

Table 3 shows the results for selected optimization levels of the benchmark *bubblesort*. Column three of the table shows the highest mean value of the corresponding function over all cycle windows in per cent of the threshold.

While in *bubblesort O0* all functions are below the threshold, in *bubblesort O1* the function *sort* and *init* produce a critical peak. In *bubblesort O1 no-tree-dominator-opts* the function *sort* is again under the threshold, but *init* still

Table 3. Results of *bubblesort* for different optimization levels on function level

| function | Cycles | Max. Mean Power [%] | Cycles | Max. Mean Power [%] |
|----------|--------------------------------------|---------------------|---------------------------|---------------------|
| | bubblesort O0 | | bubblesort O1 | |
| init | 2166 | 94.36 | 330 | 103.97 |
| sort | 355290 | 96.47 | 52193 | 102.94 |
| check | 108 | 90.10 | 37 | 97.29 |
| main | 64 | 87.97 | 28 | 95.81 |
| all | 357628 | 96.47 | 52782 | 103.97 |
| | bubblesort O1 no-tree-dominator-opts | | bubblesort peak optimized | |
| init | 421 | 102.84 | 734 | 94.36 |
| sort | 56280 | 99.14 | 56280 | 99.14 |
| check | 8 | 82.39 | 17 | 97.29 |
| main | 42 | 91.60 | 45 | 95.81 |
| all | 56751 | 102.24 | 57076 | 99.14 |

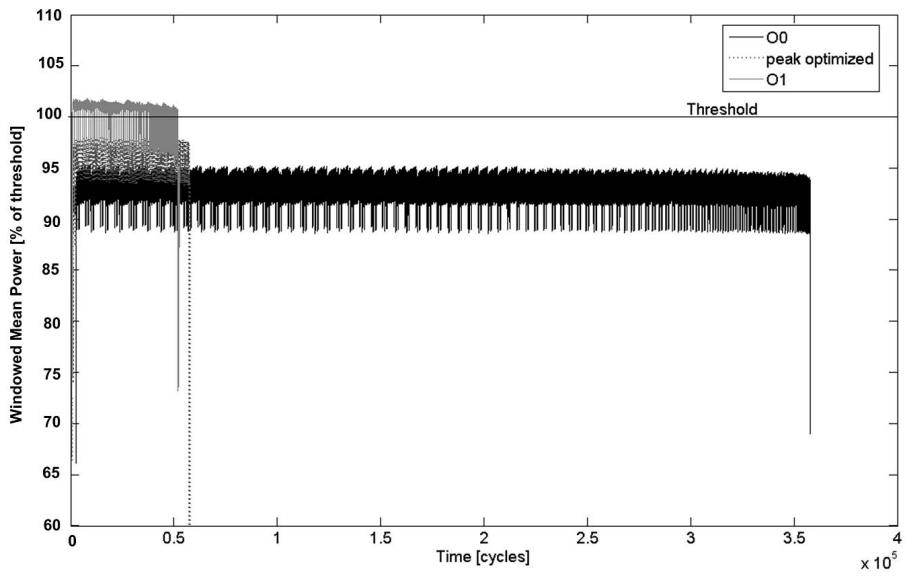


Fig. 5. Power profile with O0, O1 and the resulting code of the peak elimination framework for *bubblesort*

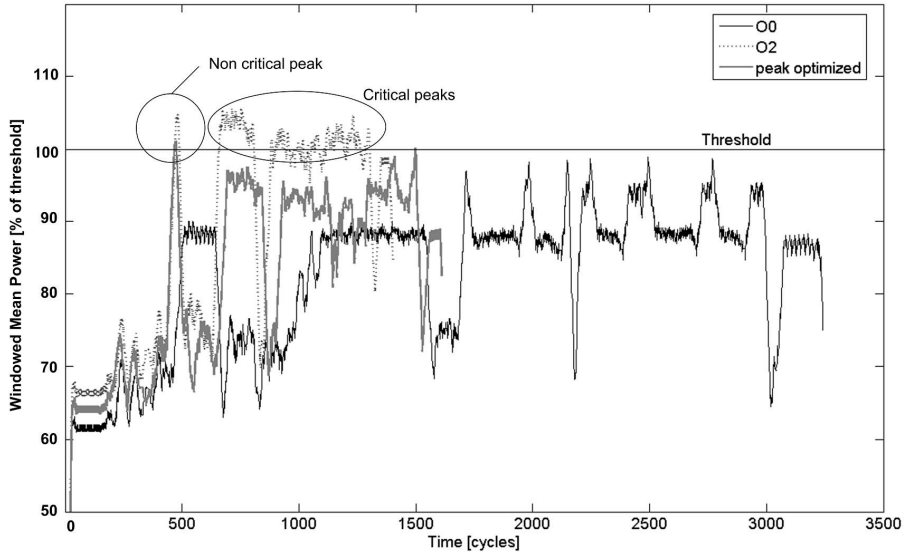


Fig. 6. Power profile with O0, O2 and the resulting code of the peak elimination framework for *quicksort*

remains above. The optimized configuration is thus composed of *init* with *O0*, *sort* with *O1 no-tree-dominator-opts* and *main* and *check* with *O1*. The peak optimized code was obtained after 13 compile cycles. The power profile of the peak optimized code is depicted in Fig. 5. The whole power profile is below the threshold. As a tradeoff we lose 1.2% of the performance compared to the *O1*-optimized code, but still we only need 16% of the cycles compared to the *O0*-level.

For the benchmark *quicksort* the power profile is depicted in Fig. 6. The first marked peak is not critical for the system caused by his shortness and does not have to be eliminated. The second marked region in the *O2*-profile contains several longer peaks, which are critical for the system. It was possible to reduce these peaks by lowering the optimization level of the corresponding functions. In this case we lose 3.9% of the performance compared to the *O2*-optimized code, but still we only need 47% of the cycles compared to the *O0*-level.

6 Conclusion

The elimination of power peaks in the power profile of smart cards represents an important aspect for better system stability. In this paper we presented a new approach to eliminate power peaks of the power profile of an application executed on an embedded processor. The results have shown that the compiler can be used to eliminate critical peaks. Iterative compiling can be used to find the optimal tradeoff between performance and system stability. To also allow for the elimination of hardware peaks, in a next step the framework will be enhanced by further peak elimination methods like presented in section 3.

Acknowledgments

This work was funded by the Austrian Federal Ministry for Transport, Innovation, and Technology under the FFG contract FFG 810124.

References

1. Haid, J., Kargl, W., Leutgeb, T., Scheiblhofer, D.: Power Management for RF-Powered vs. Battery-Powered Devices. In: Proceedings of Workshop on Wearable and Pervasive Computing, Graz, Austria (2005)
2. Rothbart, K., Neffe, U., Steger, C., Weiss, R., Rieger, E., Muehlberger, A.: Power consumption profile analysis for security attack simulation in smart cards at high abstraction level. In: EMSOFT 2005. Proceedings of the 5th ACM international conference on Embedded software, Jersey City, NJ, USA, pp. 214–217. ACM Press, New York (2005)
3. Tiwari, V., Malik, S., Wolfe, A.: Power analysis of embedded software: a first step towards software power minimization. In: ICCAD 1994. Proceedings of the 1994 IEEE/ACM international conference on Computer-aided design, IEEE Computer Society Press, Los Alamitos (1994)

4. Tiwari, V., Malik, S., Wolfe, A., Lee, M.T.C.: Instruction level power analysis and optimization of software. *J. VLSI Signal Process. Syst.* 13(2-3), 223–238 (1996)
5. Knijnenburg, P.M.W., Kisuki, T., O'Boyle, M.F.P.: Iterative compilation, 171–187 (2002)
6. Kisuki, T., Knijnenburg, P.M.W., O'Boyle, M.F.P.: Combined Selection of Tile Sizes and Unroll Factors Using Iterative Compilation. In: *PACT 2000. Proceedings of the 2000 International Conference on Parallel Architectures and Compilation Techniques*, Washington, DC, USA, p. 237. IEEE Computer Society, Los Alamitos (2000)
7. Fursin, G., O'Boyle, M., Knijnenburg, P.: Evaluating Iterative Compilation, 305–315 (2002)
8. Cooper, K.D., Grosul, A., Harvey, T.J., Reeves, S., Subramanian, D., Torczon, L., Waterman, T.: ACME: adaptive compilation made efficient. In: *LCTES 2005. Proceedings of the 2005 ACM SIGPLAN/SIGBED conference on Languages, compilers, and tools for embedded systems*, Chicago, Illinois, USA, pp. 69–77. ACM Press, New York (2005)
9. Cooper, K.D., Schielke, P.J., Subramanian, D.: Optimizing for reduced code space using genetic algorithms. In: *LCTES 1999. Proceedings of the ACM SIGPLAN 1999 workshop on Languages, compilers, and tools for embedded systems*, Atlanta, Georgia, United States, pp. 1–9. ACM Press, New York (1999)
10. Cooper, K.D., Subramanian, D., Torczon, L.: Adaptive Optimizing Compilers for the 21st Century. *J. Supercomput.* 23(1), 7–22 (2002)
11. Kulkarni, P., Zhao, W., Moon, H., Cho, K., Whalley, D., Davidson, J., Bailey, M., Paek, Y., Gallivan, K.: Finding effective optimization phase sequences. *SIGPLAN Not.* 38(7), 12–23 (2003)
12. Fursin, G., Cohen, A.: Building a Practical Iterative Interactive Compiler. In: De Bosschere, K., Kaeli, D., Stenström, P., Whalley, D., Ungerer, T. (eds.) *HiPEAC 2007. LNCS*, vol. 4367, Springer, Heidelberg (2007)
13. Gheorghita, S., Corporaal, H., Basten, T.: Using Iterative Compilation to Reduce Energy Consumption. In: *ASCI 2004. Proceedings of the 10th Annual Conference of the Advanced School for Computing and Imaging*, Delft, The Netherlands, pp. 197–202 (2004)
14. Neffe, U., Rothbart, K., Steger, C., Weiss, R., Rieger, E., Muehlberger, A.: A Flexible and Accurate Model of an Instruction-Set Simulator for Secure Smart Card Software Design. In: Macii, E., Paliouras, V., Koufopavlou, O. (eds.) *PATMOS 2004. LNCS*, vol. 3254, pp. 491–500. Springer, Heidelberg (2004)

Simultaneous Operation Scheduling and Operation Delay Selection to Minimize Cycle-by-Cycle Power Differential

Wei-Ting Yen, Shih-Hsu Huang, and Chun-Hua Cheng

Department of Electronic Engineering,
Chung Yuan Christian University, Chung Li, Taiwan, R.O.C.
shhuang@cycu.edu.tw

Abstract. The cycle-by-cycle power differential determines the noise introduced due to inductive ground bounce. However, very few attentions are paid to minimize the cycle-by-cycle power differential in high-level synthesis stage. In this paper, we investigate the simultaneous application of operation scheduling and operation delay selection for minimizing the cycle-by-cycle power differential. An integer linear programming (ILP) approach is proposed to formally formulate this problem. Benchmark data consistently show that our approach can minimize the cycle-by-cycle power differential within an acceptable run time. Compared with previous work, the relative improvement of our approach achieves 44.8%.

Keywords: Integer Linear Programming, High-Level Synthesis, Data-Path Synthesis, Low Power, Operation Scheduling, Cycle-by-cycle Power Differential.

1 Introduction

In low-power designs for battery driven portable applications, average power, peak power, and cycle-by-cycle peak power differential are all equally important considerations. However, most previous high-level synthesis approaches [1-6] focus on the minimization of average power and/or peak power. To the best of our knowledge, [7] was the only high-level synthesis approach to the minimization of cycle-by-cycle power differential. In fact, the cycle-by-cycle power differential determines the noise introduced due to inductive ground bounce. Therefore, the minimization of cycle-by-cycle power differential is crucial in designing efficient and reliable integrated circuits.

In high-level synthesis stage [8], a behavior description is translated into a control-data flow graph (CDFG), where each node corresponds to an operation, and each directed edge corresponds to data dependency or control relation. Under specified design constraints (timing and resource), operation scheduling [7-10] is to assign each operation in the CDFG to a specific control step to start its execution. It has been recognized that operation scheduling greatly influences all quality aspects of the final implementation. Therefore, according to Gajski [8], operation scheduling is “perhaps

the most important task in high-level synthesis". In [7], an integer linear programming (ILP) approach is proposed to formulate the problem of operation scheduling for the minimization of cycle-by-cycle power differential. In fact, up to now, [7] was the only attempt to reduce the cycle-by-cycle power differential via operation scheduling.

Different from previous work [7], in this paper, we combine operation scheduling and operation delay selection to minimize the cycle-by-cycle power differential. We find that, by slowing down non-critical operations, the cycle-by-cycle power differential can be further minimized. Therefore, based on that observation, we propose an ILP approach to formally formulate the simultaneous application of operation scheduling and operation delay selection. Compared with previous work [7], experimental results demonstrate that our approach can reduce the cycle-by-cycle power differential up to 44.8%.

The organization of this paper is as below. Section 2 gives the problem description. Section 3 describes our approach, and presents the ILP formulation. Section 4 demonstrates the experimental results. Finally, some concluding remarks are given in Section 5.

2 Motivation

Kindly assure that the Contact Volume Editor is given the name and email address of the contact author for your paper. The Contact Volume Editor uses these details to compile a list for our production department at SPS in India. Once the files have been worked upon, SPS sends a copy of the final pdf of each paper to its contact author. The contact author is asked to check through the final pdf to make sure that no errors have crept in during the transfer or preparation of the files. This should not be seen as an opportunity to update or copyedit the papers, which is not possible due to time constraints. Only errors introduced during the preparation of the files will be corrected.

This round of checking takes place about two weeks after the files have been sent to the Editorial by the Contact Volume Editor, i.e., roughly seven weeks before the start of the conference for conference proceedings, or seven weeks before the volume leaves the printer's, for post-proceedings. If SPS does not receive a reply from a particular contact author, within the timeframe given, then it is presumed that the author has found no errors in the paper. The tight publication schedule of LNCS does not allow SPS to send reminders or search for alternative email addresses on the Internet.

In some cases, it is the Contact Volume Editor that checks all the pdfs. In such cases, the authors are not involved in the checking phase.

We use the data flow graph shown in Figure 1 to illustrate our motivation. The notation $>$ denotes the control operations, the notation $+$ denotes the addition operations, the notation $-$ denotes the subtraction operations, and the notation $*$ denotes the multiplication operations.

Assume that the power consumptions of control operation, addition operation, subtraction operation, and multiplication operation are 3mW, 3mW, 3mW, and 20mW, respectively. Figure 1(a) shows a scheduled DFG under the constraint of 1 multiplier, 1 adder, and 3 control steps. The peak power consumptions at control steps

1, 2, and 3 are 3 mW, 23 mW, and 20 mW, respectively. Analysis of the Figure 1(a) reveals that largest cycle-by-cycle is 20 mW.

For each operation, we assume that the power consumption is uniformly distributed to each control step when it executes. Suppose that the power consumption of a multiplication operation is 20mW. Then, the power consumption of each control step is 20 mW if the multiplication operation is executed within one control step; the power consumption of each control step is 10 mW if the multiplication operation is executed within two control steps; the power consumption of each control step is 20/3 mW if the multiplication operation is executed within three control steps; and so on. Based on that observation, if we can slow down non-critical operations, the cycle-by-cycle power differential can be further minimized. For example, in Figure 1(a), operation o4 is a non-critical operation. Therefore, we can slow down operation o4. As a result, we obtain another scheduled DFG as shown in Figure 1(b). The peak power consumptions at control steps 1, 2, and 3 are 13 mW, 13 mW, and 20 mW, respectively. Analysis of the Figure 1(b) reveals that largest cycle-by-cycle power differential is only 7 mW.

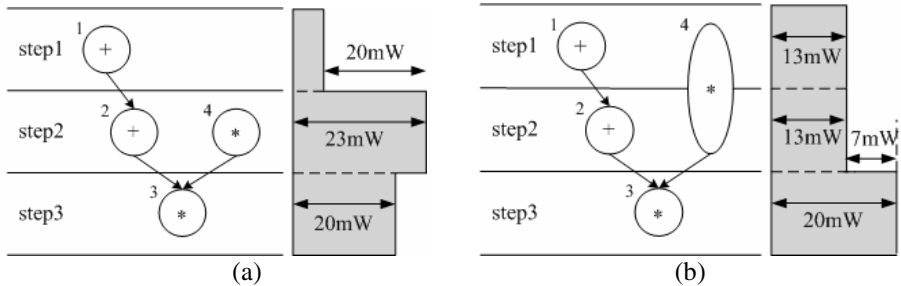


Fig. 1. A motivational example

3 The Formulations

In our ILP formulations, we use the notation $x_{i,j,s}$ to denote a binary variable (i.e., an 0-1 integer variable). Binary variable $x_{i,j,s} = 1$, if and only if operation o_i is scheduled into control step j and the slack of operation o_i is exactly s clock cycles; otherwise, binary variable $x_{i,j,s} = 0$. Clearly, we have $1 \leq i \leq n$, $1 \leq j \leq t$ and $0 \leq s \leq t-1$, where n is the number of operations in the data flow graph and t is the total number of control steps. Thus, intuitively, the total number of binary variables is $n \cdot t^2$. However, in fact, from the ASAP (as soon as possible) and ALAP (as late as possible) schedules, we can find that a lot of binary variables are redundant since their values are definitely 0. Therefore, we can prune these redundant binary variables without sacrificing the accuracy of the solution.

The constants used in our ILP formulations are as below.

The value w_i denotes the power consumption of operation o_i .

The value s denotes delay time steps of each operation.

The value t denotes the total number of control steps.

The value n denotes the number of operations in the data flow graph.

The delay of each operation o_i corresponds to D_i clock cycles.

The value E_i denotes the earliest possible control step of operation o_i . Note that we can use the ASAP calculation to determine the value E_i for each operation o_i .

The value L_i denotes the latest possible control step of operation o_i . Note that, given the total number of control steps, we can use the ALAP calculation to determine the value L_i for each operation o_i .

We use FU_p to denote functional unit of type p , and we say $o_i \in FU_p$ if and only if operation o_i and o_k can be executed by FU_p .

The value M_p is the number of functional units of type p .

The cycle-by-cycle power differential minimization problem can be formulated as below.

Minimize power_differential (1)

Subject to

For each control step c and each operation o_i, o_k and $1 \leq i, k \leq n, 1 \leq c \leq t-1$

$$\begin{aligned}
 -power_differential &\leq \sum_{j=E_i}^c \sum_{s=c-(j+D_i-1)}^{L_i-j} \frac{w_i}{s+1} X_{i,j,s} - \\
 \sum_{j=E_k}^{c+1} \sum_{s=c+1-(j+D_i-1)}^{L_k-j} \frac{w_k}{s+1} X_{k,j,s} &\leq power_differential
 \end{aligned} \tag{2}$$

For each operation o_i and $1 \leq i \leq n$

$$\sum_{j=E_i}^{L_i} \sum_{s=0}^{L_i-j} X_{i,j,s} = 1 \tag{3}$$

For each data dependency relation $o_i \rightarrow o_l$ and $1 \leq i \leq n, 1 \leq l \leq n$

$$\sum_{j=E_i}^{L_i} \sum_{s=0}^{L_i-j} (j+D+s-1) X_{i,j,s} < \sum_{j=E_l}^{L_l} \sum_{s=0}^{L_l-j} j X_{l,j,s} \tag{4}$$

For each control step c and each type of function unit FU_p

$$\sum_{o_i \in FU_p} \sum_{j=E_i}^c \sum_{s=c-(j+D_i-1)}^{L_i-j} X_{i,j,s} \leq M_p \tag{5}$$

Formula 1 defines the objective function. Formula 2 and Formula 3 describe peak power and peak power differential respectively. Formula 4 states the constraint that every operation must be scheduled to a control step. Formula 5 ensures that the data dependency relationships are preserved. Formula 6 states that the number of resources, type k , used in any control step should be less than or equal to the allocated resources M_p .

We use the HAL example [9] as shown in Figure 2 to illustrate the ILP formulations. The delay of each operation is 1 control step, i.e., $D_i = 1$ for $i = 1, 2, \dots, 11$. The timing constraint is 5 control steps; in other words, the total number of control steps is 5. Figure 2(a) and (b) show the ASAP and ALAP schedules of this

example. According to the ASAP and ALAP schedules, we can prune all the redundant binary variables. Table 1 tabulates all the necessary (i.e., irredundant) binary variables associated with each operation.

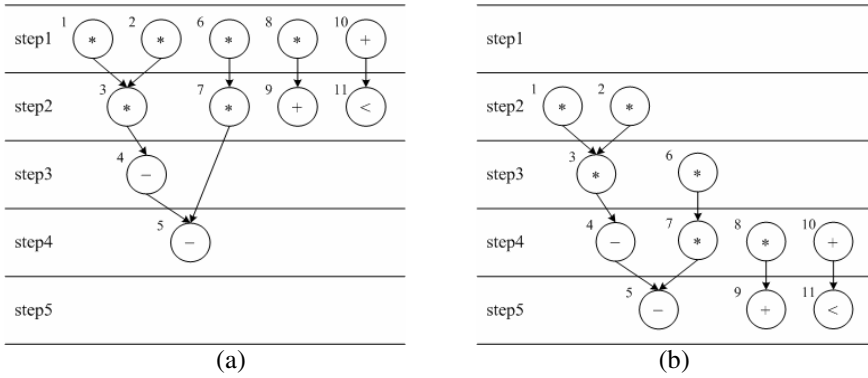


Fig. 2. HAL example. (a) ASAP schedule. (b) ALAP schedule.

Table 1. The binary variables associated with each operation

| Operation | Associated Binary Variables |
|-----------------|--|
| O ₁ | X _{1,1,0} , X _{1,1,1} , X _{1,2,0} |
| O ₂ | X _{2,1,0} , X _{2,1,1} , X _{2,2,0} |
| O ₃ | X _{3,2,0} , X _{3,2,1} , X _{3,3,0} |
| O ₄ | X _{4,3,0} , X _{4,3,1} , X _{4,4,0} |
| O ₅ | X _{5,4,0} , X _{5,4,1} , X _{5,5,0} |
| O ₆ | X _{6,1,0} , X _{6,1,1} , X _{6,1,2} , X _{6,2,0} , X _{6,2,1} , X _{6,3,0} |
| O ₇ | X _{7,2,0} , X _{7,2,1} , X _{7,2,2} , X _{7,3,0} , X _{7,3,1} , X _{7,4,0} |
| O ₈ | X _{8,1,0} , X _{8,1,1} , X _{8,1,2} , X _{8,1,3} , X _{8,2,0} , X _{8,2,1} , X _{8,2,2} , X _{8,3,0} , X _{8,3,1} , X _{8,4,0} |
| O ₉ | X _{9,2,0} , X _{9,2,1} , X _{9,2,2} , X _{9,2,3} , X _{9,3,0} , X _{9,3,1} , X _{9,3,2} , X _{9,4,0} , X _{9,4,1} , X _{9,5,0} |
| O ₁₀ | X _{10,1,0} , X _{10,1,1} , X _{10,1,2} , X _{10,1,3} , X _{10,2,0} , X _{10,2,1} , X _{10,2,2} , X _{10,3,0} , X _{10,3,1} , X _{10,4,0} |
| O ₁₁ | X _{11,2,0} , X _{11,2,1} , X _{11,2,2} , X _{11,2,3} , X _{11,3,0} , X _{11,3,1} , X _{11,3,2} , X _{11,4,0} , X _{11,4,1} , X _{11,5,0} |

Assume that there are two types of functional units: the multiplier (FU_1), which can execute the multiplication operation, and the ALU (FU_2), which can execute other operations. Now we can construct the ILP formulations as below.

Formula 2. Using an example to illustrate peak power and peak power differential for control step 4 to control step 5. Thus, we have $-power_differential \leq (3x_{4,4,0} + 1.5x_{4,3,1} + 3x_{5,4,0} + 20x_{7,4,0} + 6.7x_{7,2,2} + 10x_{7,3,1} + 20x_{8,4,0} + 5x_{8,1,3} + 6.7x_{8,2,2} + 10x_{8,3,1} + 3x_{9,4,0} + 1x_{9,2,2} + 1.5x_{9,3,1} + 3x_{10,4,0} + 0.75x_{10,1,3} + 1x_{10,2,2} + 1.5x_{10,3,1} + 3x_{11,4,0} + 1x_{11,2,2}$

+ $1.5x_{11,3,1} + 1.5x_{5,4,1} + 1x_{9,3,2} + 0.75x_{9,2,3} + 1.5x_{9,4,1} + 0.75x_{11,2,3} + 1x_{11,3,2} + 1.5x_{11,4,1}$) - $(3x_{5,5,0} + 3x_{9,5,0} + 3x_{11,5,0} + 1.5x_{5,4,1} + 1x_{9,3,2} + 0.75x_{9,2,3} + 1.5x_{9,4,1} + 0.75x_{11,2,3} + 1x_{11,3,2} + 1.5x_{11,4,1}) \leq \text{power_differential}$. All the constraints due to Formula 2 are listed in the following.

$$-\text{power_differential} \leq (20x_{1,1,0} + 10x_{1,1,1} + 20x_{2,1,0} + 10x_{2,1,1} + 20x_{6,1,0} + 10x_{6,1,1} + 6.7x_{6,1,2} + 20x_{8,1,0} + 10x_{8,1,1} + 6.7x_{8,1,2} + 5x_{8,1,3} + 3x_{10,1,0} + 1.5x_{10,1,1} + 1x_{10,1,2} + 0.75x_{10,1,3}) - (10x_{1,1,1} + 20x_{1,2,0} + 10x_{2,1,1} + 20x_{2,2,0} + 20x_{3,2,0} + 10x_{3,2,1} + 10x_{6,1,1} + 6.7x_{6,1,2} + 20x_{6,2,0} + 10x_{6,2,1} + 20x_{7,2,0} + 10x_{7,2,1} + 6.7x_{7,2,2} + 10x_{8,1,1} + 6.7x_{8,1,2} + 5x_{8,1,3} + 20x_{8,2,0} + 10x_{8,2,1} + 6.7x_{8,2,2} + 3x_{9,2,0} + 1.5x_{9,2,1} + 1x_{9,2,2} + 0.75x_{9,2,3} + 3x_{10,2,0} + 1.5x_{10,1,1} + 1x_{10,1,2} + 0.75x_{10,1,3} + 1.5x_{10,2,1} + 1x_{10,2,2} + 3x_{11,2,0} + 1.5x_{11,2,1} + 1x_{11,2,2} + 0.75x_{11,2,3}) \leq \text{power_differential};$$

$$-\text{power_differential} \leq (10x_{1,1,1} + 20x_{1,2,0} + 10x_{2,1,1} + 3x_{9,2,0} + 20x_{2,2,0} + 20x_{3,2,0} + 10x_{3,2,1} + 10x_{6,1,1} + 6.7x_{6,1,2} + 20x_{6,2,0} + 10x_{6,2,1} + 20x_{7,2,0} + 10x_{7,2,1} + 6.7x_{7,2,2} + 10x_{8,1,1} + 5x_{8,1,3} + 6.7x_{8,1,2} + 20x_{8,2,0} + 10x_{8,2,1} + 6.7x_{8,2,2} + 1.5x_{9,2,1} + 1x_{9,2,2} + 0.75x_{9,2,3} + 1.5x_{10,1,1} + 1x_{10,1,2} + 0.75x_{10,1,3} + 3x_{10,2,0} + 1.5x_{10,2,1} + 1x_{10,2,2} + 3x_{11,2,0} + 1.5x_{11,2,1} + 1x_{11,2,2} + x_{11,2,3}) - (10x_{3,2,1} + 20x_{3,3,0} + 6.7x_{6,1,2} + 10x_{6,2,1} + 20x_{6,3,0} + 10x_{7,2,1} + 6.7x_{7,2,2} + 20x_{7,3,0} + 10x_{7,3,1} + 6.7x_{8,1,2} + 5x_{8,1,3} + 10x_{8,2,1} + 6.7x_{8,2,2} + 20x_{8,3,0} + 10x_{8,3,1} + 3x_{4,3,0} + 1.5x_{4,3,1} + 1.5x_{9,2,1} + 1x_{9,2,2} + 0.75x_{9,2,3} + 3x_{9,3,0} + 1.5x_{9,3,1} + 1x_{9,3,2} + 1x_{10,1,2} + 0.75x_{10,1,3} + 1.5x_{10,2,1} + 1x_{10,2,2} + 3x_{10,3,0} + 1.5x_{10,3,1} + 1.5x_{11,2,1} + 1x_{11,2,2} + 0.75x_{11,2,3} + 3x_{11,3,0} + 1.5x_{11,3,1} + 1x_{11,3,2}) \leq \text{power_differential};$$

$$-\text{power_differential} \leq (10x_{3,2,1} + 20x_{3,3,0} + 6.7x_{6,1,2} + 10x_{6,2,1} + 20x_{6,3,0} + 10x_{7,2,1} + 6.7x_{7,2,2} + 20x_{7,3,0} + 10x_{7,3,1} + 6.7x_{8,1,2} + 5x_{8,1,3} + 10x_{8,2,1} + 6.7x_{8,2,2} + 20x_{8,3,0} + 10x_{8,3,1} + 3x_{4,3,0} + 1.5x_{4,3,1} + 1.5x_{9,2,1} + 1x_{9,2,2} + 0.75x_{9,2,3} + 3x_{9,3,0} + 1.5x_{9,3,1} + 1x_{9,3,2} + 1x_{10,1,2} + 0.75x_{10,1,3} + 1.5x_{10,2,1} + 1x_{10,2,2} + 3x_{10,3,0} + 1.5x_{10,3,1} + 1.5x_{11,2,1} + 1x_{11,2,2} + 3x_{11,3,0} + 1x_{11,3,2} + 0.75x_{11,2,3} + 1.5x_{11,3,1}) - (20x_{3,3,0} + 10x_{3,2,1} + 3x_{4,3,0} + 20x_{6,3,0} + 6x_{6,1,2} + 10x_{6,2,1} + 20x_{7,3,0} + 10x_{7,2,1} + 20x_{8,3,0} + 6x_{8,1,2} + 10x_{8,2,1} + 3x_{9,3,0} + 1x_{9,2,1} + 3x_{10,3,0} + 1x_{10,1,2} + 1x_{10,2,1} + 3x_{11,3,0} + 1x_{11,2,1}) \leq \text{power_differential};$$

$$-\text{power_differential} \leq (3x_{4,4,0} + 1.5x_{4,3,1} + 3x_{5,4,0} + 20x_{7,4,0} + 6.7x_{7,2,2} + 10x_{7,3,1} + 20x_{8,4,0} + 5x_{8,1,3} + 6.7x_{8,2,2} + 10x_{8,3,1} + 3x_{9,4,0} + 1x_{9,2,2} + 1.5x_{9,3,1} + 3x_{10,4,0} + 0.75x_{10,1,3} + 1x_{10,2,2} + 1.5x_{10,3,1} + 3x_{11,4,0} + 1x_{11,2,2} + 1.5x_{11,3,1} + 1.5x_{5,4,1} + 1x_{9,3,2} + 0.75x_{9,2,3} + 1.5x_{9,4,1} + 0.75x_{11,2,3} + 1x_{11,3,2} + 1.5x_{11,4,1}) - (3x_{5,5,0} + 3x_{9,5,0} + 3x_{11,5,0} + 1.5x_{5,4,1} + 1x_{9,3,2} + 0.75x_{9,2,3} + 1.5x_{9,4,1} + 0.75x_{11,2,3} + 1x_{11,3,2} + 1.5x_{11,4,1}) \leq \text{power_differential};$$

Formula 3. Using operation o_{10} as an example, there is exactly one binary variable is true among all the six binary variables associated with operation o_{10} . Thus, we have $x_{10,1,0} + x_{10,1,1} + x_{10,1,2} + x_{10,1,3} + x_{10,2,0} + x_{10,2,1} + x_{10,2,2} + x_{10,3,0} + x_{10,3,1} + x_{10,4,0} = 1$. All the constraints due to Formula 3 are listed in the following.

$$\begin{aligned} x_{1,1,0} + x_{1,1,1} + x_{1,2,0} &= 1; \\ x_{2,1,0} + x_{2,1,1} + x_{2,2,0} &= 1; \\ x_{3,2,0} + x_{3,2,1} + x_{3,3,0} &= 1; \\ x_{4,3,0} + x_{4,3,1} + x_{4,4,0} &= 1; \\ x_{5,4,0} + x_{5,4,1} + x_{5,5,0} &= 1; \\ x_{6,1,0} + x_{6,1,1} + x_{6,1,2} + x_{6,2,0} + x_{6,2,1} + x_{6,3,0} &= 1; \\ x_{7,2,0} + x_{7,2,1} + x_{7,2,2} + x_{7,3,0} + x_{7,3,1} + x_{7,4,0} &= 1; \end{aligned}$$

$$\begin{aligned}
x_{8,1,0} + x_{8,1,1} + x_{8,1,2} + x_{8,1,3} + x_{8,2,0} + x_{8,2,1} + x_{8,2,2} + x_{8,3,0} + x_{8,3,1} + x_{8,4,0} &= I; \\
x_{9,2,0} + x_{9,2,1} + x_{9,2,2} + x_{9,2,3} + x_{9,3,0} + x_{9,3,1} + x_{9,3,2} + x_{9,4,0} + x_{9,4,1} + x_{9,5,0} &= I; \\
x_{10,1,0} + x_{10,1,1} + x_{10,1,2} + x_{10,1,3} + x_{10,2,0} + x_{10,2,1} + x_{10,2,2} + x_{10,3,0} + x_{10,3,1} + x_{10,4,0} &= I; \\
x_{11,2,0} + x_{11,2,1} + x_{11,2,2} + x_{11,2,3} + x_{11,3,0} + x_{11,3,1} + x_{11,3,2} + x_{11,4,0} + x_{11,4,1} + x_{11,5,0} &= I;
\end{aligned}$$

Formula 4. Using the data dependency relation of $o_1 \rightarrow o_3$ as an example, operation o_3 can be executed if and only if operation o_1 has completed its execution. If operation o_1 is schedule into control step 1 with zero slack, operation o_3 can be scheduled into control step 2 with the slack of at most one clock cycle. If operation o_1 is scheduled into control step 1 with the slack of one clock cycle or operation o_1 is scheduled into control step 2 with zero slack, operation o_3 can only be scheduled into control step 3 with zero slack. Thus, we have $x_{1,1,0} + 2x_{1,1,1} + 2x_{1,2,0} < 2x_{3,2,0} + 2x_{3,2,1} + 3x_{3,3,0}$. All the constraints due to Formula 4 are listed in the following.

$$\begin{aligned}
x_{1,1,0} + 2x_{1,1,1} + 2x_{1,2,0} &< 2x_{3,2,0} + 2x_{3,2,1} + 3x_{3,3,0}; \\
x_{2,1,0} + 2x_{2,1,1} + 2x_{2,2,0} &< 2x_{3,2,0} + 2x_{3,2,1} + 3x_{3,3,0}; \\
2x_{3,2,0} + 3x_{3,2,1} + 3x_{3,3,0} &< 3x_{4,3,0} + 3x_{4,3,1} + 4x_{4,4,0}; \\
3x_{4,3,0} + 4x_{4,3,1} + 4x_{4,4,0} &< 4x_{5,4,0} + 4x_{5,4,1} + 5x_{5,5,0}; \\
x_{6,1,0} + 2x_{6,1,1} + 3x_{6,1,2} + 2x_{6,2,0} + 3x_{6,2,1} + 3x_{6,3,0} &< 2x_{7,2,0} + 2x_{7,2,1} + 2x_{7,2,2} + 3x_{7,3,0} + \\
&3x_{7,3,1} + 4x_{7,4,0}; \\
2x_{7,2,0} + 3x_{7,2,1} + 4x_{7,2,2} + 3x_{7,3,0} + 4x_{7,3,1} + 4x_{7,4,0} &< 4x_{5,4,0} + 4x_{5,4,1} + 5x_{5,5,0}; \\
x_{8,1,0} + 2x_{8,1,1} + 3x_{8,1,2} + 4x_{8,1,3} + 2x_{8,2,0} + 3x_{8,2,1} + 4x_{8,2,2} + 3x_{8,3,0} + 4x_{8,3,1} + 4x_{8,4,0} &< \\
2x_{9,2,0} + 2x_{9,2,1} + 2x_{9,2,2} + 2x_{9,2,3} + 3x_{9,3,0} + 3x_{9,3,1} + 3x_{9,3,2} + 4x_{9,4,0} + 4x_{9,4,1} + 5x_{9,5,0}; \\
x_{10,1,0} + 2x_{10,1,1} + 3x_{10,1,2} + 4x_{10,1,3} + 2x_{10,2,0} + 3x_{10,2,1} + 4x_{10,2,2} + 3x_{10,3,0} + 4x_{10,3,1} + \\
4x_{10,4,0} &< 2x_{11,2,0} + 2x_{11,2,1} + 2x_{11,2,2} + 2x_{11,2,3} + 3x_{11,3,0} + 3x_{11,3,1} + 3x_{11,3,2} + 4x_{11,4,0} + \\
4x_{11,4,1} + 5x_{11,5,0};
\end{aligned}$$

Formula 5. Consider that there are four multiplication operations o_3 , o_6 , o_7 and o_8 can be scheduled into control step 3. However, the maximum number of multiplication operations that can be scheduled into control step 3 is constrained by the number of multipliers (i.e., M_1). Thus, we have $x_{3,2,1} + x_{3,3,0} + x_{6,1,2} + x_{6,2,1} + x_{6,3,0} + x_{7,2,1} + x_{7,2,2} + x_{7,3,0} + x_{7,3,1} + x_{8,1,2} + x_{8,1,3} + x_{8,2,1} + x_{8,2,2} + x_{8,3,0} + x_{8,3,1} \leq M_1$. Suppose that we are given three multipliers and three ALUs; in other words, $M_1 = 3$ and $M_2 = 3$. All the constraints due to Formula 5 are listed in the following.

$$\begin{aligned}
x_{1,1,0} + x_{1,1,1} + x_{2,1,0} + x_{2,1,1} + x_{6,1,0} + x_{6,1,1} + x_{6,1,2} + x_{8,1,0} + x_{8,1,1} + x_{8,1,2} + x_{8,1,3} &\leq 3; \\
x_{1,1,1} + x_{1,2,0} + x_{2,1,1} + x_{2,2,0} + x_{3,2,0} + x_{3,2,1} + x_{6,1,1} + x_{6,1,2} + x_{6,2,0} + x_{6,2,1} + x_{7,2,0} + \\
x_{7,2,1} + x_{7,2,2} + x_{8,1,1} + x_{8,1,2} + x_{8,1,3} + x_{8,2,0} + x_{8,2,1} + x_{8,2,2} &\leq 3; \\
x_{3,2,1} + x_{3,3,0} + x_{6,1,2} + x_{6,2,1} + x_{6,3,0} + x_{7,2,1} + x_{7,2,2} + x_{7,3,0} + x_{7,3,1} + x_{8,1,2} + x_{8,1,3} + \\
x_{8,2,1} + x_{8,2,2} + x_{8,3,0} + x_{8,3,1} &\leq 3; \\
x_{7,2,2} + x_{7,3,1} + x_{7,4,0} + x_{8,1,3} + x_{8,2,2} + x_{8,3,1} + x_{8,4,0} &\leq 3; \\
x_{10,1,0} + x_{10,1,1} + x_{10,1,2} + x_{10,1,3} &\leq 3; \\
x_{9,2,0} + x_{9,2,1} + x_{9,2,2} + x_{9,2,3} + x_{10,1,1} + x_{10,1,2} + x_{10,1,3} + x_{10,2,0} + x_{10,2,1} + x_{10,2,2} + x_{11,2,0} + \\
x_{11,2,1} + x_{11,2,2} + x_{11,2,3} &\leq 3; \\
x_{4,3,0} + x_{4,3,1} + x_{9,2,1} + x_{9,2,2} + x_{9,2,3} + x_{9,3,0} + x_{9,3,1} + x_{9,3,2} + x_{10,1,2} + x_{10,1,3} + x_{10,2,1} + \\
x_{10,2,2} + x_{10,3,0} + x_{10,3,1} + x_{11,2,1} + x_{11,2,2} + x_{11,2,3} + x_{11,3,0} + x_{11,3,1} + x_{11,3,2} &\leq 3; \\
x_{4,3,1} + x_{4,4,0} + x_{5,4,0} + x_{5,4,1} + x_{9,2,2} + x_{9,2,3} + x_{9,3,1} + x_{9,3,2} + x_{9,4,0} + x_{9,4,1} + x_{10,1,3} + \\
x_{10,2,2} + x_{10,3,1} + x_{10,4,0} + x_{11,2,2} + x_{11,2,3} + x_{11,3,1} + x_{11,3,2} + x_{11,4,0} + x_{11,4,1} &\leq 3; \\
x_{5,4,1} + x_{5,5,0} + x_{9,2,3} + x_{9,3,2} + x_{9,4,1} + x_{9,5,0} + x_{11,2,3} + x_{11,3,2} + x_{11,4,1} + x_{11,5,0} &\leq 3;
\end{aligned}$$

After solving these ILP formulations, we have that $x_{1,1,0} = x_{2,1,0} = x_{3,2,1} = x_{4,4,0} = x_{5,5,0} = x_{6,2,0} = x_{7,3,1} = x_{8,1,3} = x_{9,5,0} = x_{10,3,0} = x_{11,5,0} = 1$ and the values of other binary variables are 0. Figure 3 gives the corresponding schedule. The cycle-by-cycle power differential is 10mW.

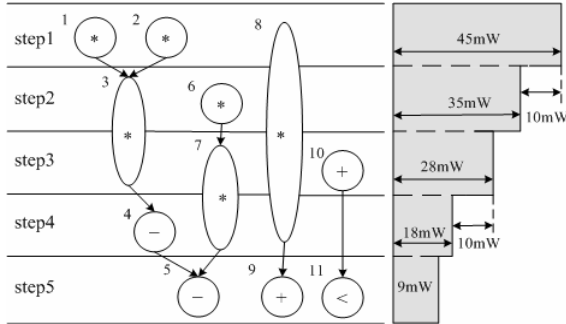


Fig. 3. Our result

4 Experimental Results

We use the Extended LINGO Release 8.0 to solve the ILP formulations on a personal computer with P4-3.3GHz CPU and 1024M Bytes RAM. Five benchmark circuits,

Table 2. Experimental results

| Circuit | Constraints | | Cycle-by-cycle power differential | | |
|---------|-----------------------|-------|-----------------------------------|------|-------|
| | Resources | Steps | [7] | Ours | Imp% |
| EF | 4 ALUs | 16 | 17 | 14 | 17.7% |
| | 4 ALUs | 17 | 17 | 11 | 35.3% |
| BF | 3 ALUs, 3 multipliers | 9 | 17 | 14 | 17.7% |
| | 3 ALUs, 3 multipliers | 10 | 14 | 7 | 50.0% |
| HAL | 3 ALUs, 3 multipliers | 5 | 14 | 10 | 28.6% |
| | 3 ALUs, 3 multipliers | 6 | 14 | 7 | 50.0% |
| AR | 4 ALUs, 4 multipliers | 9 | 34 | 28 | 17.6% |
| | 4 ALUs, 4 multipliers | 10 | 28 | 20 | 28.6% |
| IIR | 4 ALUs, 4 multipliers | 5 | 31 | 26 | 16.1% |
| | 4 ALUs, 4 multipliers | 6 | 19 | 15 | 21.1% |
| FIR | 2 ALUs, 2 multipliers | 8 | 17 | 5 | 70.6% |
| | 2 ALUs, 2 multipliers | 9 | 17 | 5 | 70.6% |
| IDCT1 | 5 ALUs, 5 multipliers | 13 | 6 | 1 | 83.3% |
| | 5 ALUs, 5 multipliers | 14 | 6 | 1 | 83.3% |
| IDCT2 | 7 ALUs, 7 multipliers | 25 | 6 | 2 | 66.6% |
| | 7 ALUs, 7 multipliers | 26 | 5 | 2 | 60.0% |

including EF [11], BF [12], HAL [9], AR [13], IIR [14], FIR [15], IDCT1 [16], and IDCT2 [16] are used to test the effectiveness of our approach. In our experiments, we assume that the power consumptions of control operation, addition operation, subtraction operation, and multiplication operation are 3mW, 3mW, 3mW, and 20mW, respectively. Given the number of multipliers, the number of ALUs, and the number of control steps, we can derive the ILP formulations for each benchmark circuit. The CPU time of each benchmark circuit is only few seconds.

For the purpose of comparisons, we also implement the ILP approach proposed in [7]. In the experiments of [7], we assume that the delay of each operation is 1 control step. Table 2 gives our experimental results. The column Resources denotes the resource constraints. The column Steps denotes the number of control steps. The column [7] denotes the largest cycle-by-cycle power differential obtained by the approach [7]. The column Ours denotes the largest cycle-by-cycle power differential obtained by our approach. The column Imp% denotes the percentage of improvement. The average improvement achieves 44.8%.

5 Conclusions

In this paper, we present an ILP formulation to model the cycle-by-cycle power differential minimization problem via operation delay selection. To the best of our knowledge, our paper is the first work that uses operation delay selection to reduce the cycle-by-cycle power differential. Benchmark data consistently show that our approach has significant cycle-by-cycle power differential reduction. Compared with previous work, our average improvement achieves 44.8%.

Acknowledgement

This work was supported in part by the National Science Council of R.O.C. under the grant number NSC 93-2220-E-033-001.

References

1. Martin, T.L., Siewiorek, D.P.: Non-Ideal Battery Properties and Low-Power Operation in Wearable Computing. In: Proc. of International Symposium on Wearable Computers, pp. 101–106 (1999)
2. Shiue, W.T.: High Level Synthesis for Peak Power Minimization using ILP. In: Proc. of IEEE International Conference on Application-Specific Systems, Architectures, and Processors, pp. 103–112 (2000)
3. Benini, L., Casterlli, G., Macii, A., Scarsi, R.: Battery-Driven Dynamic Power Management. *IEEE Design Test Computers* 13, 53–60 (2001)
4. Chen, C., Sarrafzadeh, M.: Power-Manageable Scheduling Technique for Control Dominated High-Level Synthesis. In: Proc. of IEEE Design, Automation, and Test in Europe Conference and Exhibition, pp. 1016–1020 (2002)

5. Mohanty, S.P., Ranganathan, N., Chappidi, S.K.: Peak Power Minimization through Datapath Scheduling. In: Proc. of IEEE Computer Society Annual Symposium on VLSI, pp. 121–126 (2003)
6. Huang, S.H., Cheng, C.H., Chiang, C.H., Chang, C.M.: Peak Power Minimization through Power Management Scheduling. In: Proc. of IEEE Asia and Pacific Conference on Circuits and Systems, pp. 868–971 (2006)
7. Mohanty, S.P., Ranganathan, N., Chappidi, S.K.: ILP Models for Energy and Transient Power Minimization During Behavioral Synthesis. In: Proc. of intl. Conf. on VLSI Design, pp. 745–748 (2004)
8. Gajski, D.D., Dutt, N.D., Pangrle, B.M.: Silicon Compilation (tutorial). In: Proc. of Custom Integrated Circuits Conference, pp. 102–110 (1986)
9. Hwang, C.T., Lee, J.H., Hsu, Y.C.: A Formal Approach to the Scheduling Problem in High Level Synthesis. *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems* 10(4), 464–475 (1991)
10. Faraboschi, P., Fisher, J.A., Young, C.: Instruction Scheduling for Instruction Level Parallel Processors. *Proc. of the IEEE* 89(11), 1638–1659 (2001)
11. Balakrishnan, M., Marwedel, P.: Integrated Scheduling and Binding: A Synthesis Approach for Design Space Exploration. In: Proc. of IEEE/ACM Design Automation Conference, pp. 68–74 (1989)
12. Papachristou, C.A., Konuk, H.: A Linear Program Driven Scheduling and Allocation Method Followed by an Interconnect Optimization Algorithm. In: Proc. of IEEE/ACM Design Automation Conference, pp. 77–83 (1990)
13. Ramanujam, J., Deshpande, S., Hong, J., Kandemir, M.: A Heuristic for Clock Selection in High-Level Synthesis. In: Proc. of IEEE Asia and South Pacific Design Automation Conference, pp. 414–419 (2002)
14. Kum, K.I., Sung, W.: Word-Length Optimization for High-Level Synthesis of Digital Signal Processing Systems. In: Proc. of IEEE Workshop on Signal Processing Systems, pp. 569–578 (1998)
15. Shin, D., Choi, K.: Low Power High Level Synthesis by Increasing Data Correlation. In: Proc. of IEEE International Symposium on Low Power Electronic Design, pp. 62–67 (1997)
16. Lee, C., Potkonjak, M., Maggione-Smith, W.H.: MediaBench: A Tool for Evaluating and Synthesizing Multimedia and Communications System. In: Proc. of IEEE International Symposium on Microarchitecture, pp. 330–335 (1997)

A Simple Approach to Robust Optimal Pole Assignment of Decentralized Stochastic Singularly-Perturbed Computer Controlled Systems

Kai-chao Yao

Department of Industrial Education and Technology
National Chang-hua University of Education
No. 2 Shi-Da Road, Changhua City, Taiwan
kcyao@cc.ncue.edu.tw

Abstract. This paper develops a simple algorithm for having robust optimal computer control in decentralized stochastic singularly-perturbed systems by poles assignment. This type of noise-disturbed system can be often seen in computer controlled large-scale systems such as electric power systems, communication networks, and aerospace systems. Due to that this computer controlled system possesses the fast response characteristics of the subsystems, the system analysis can be simplified by singularly perturbation methodology and the aggregation matrix is also applied to obtain faster calculation. Finally, the aggregation matrix is found out that will be an important intermediary to easily achieve the robust sub-optimal poles assignment. In the end, three steps are proposed to complete the robust sub-optimal pole assignment.

Keywords: robust, computer, pole, decentralized, stochastic, singularly-perturbed, aggregation matrix.

1 Introduction

Pole placement of large-scale systems has been a difficult task due to the high dimension of the systems. How to simplify the process of placing optimal poles is the goal of this research. In this paper, the system is concerned with decentralized stochastic singularly-perturbed computer controlled systems. Such systems are two-time scale systems. Practically, computer controlled systems are this type of systems.

There are some similar researches related to this field. G. Enea, J. Duplaix, and M. Franceschi [1] use a recursive method to achieve optimal control with aggregative pole assignment in the discrete MIMO systems. A.R. Arar and M.E. Sawan [2] propose a design method for optimal control with eigenvalue placement in a specified region; in 1997, they present the work about the relation between pole-placement and linear quadratic regulator for discrete time systems [3]. In [4], Yao studied computer control of decentralized singularly-perturbed systems, but the noise disturbing factors, fast algorithms and robustness are not concerned.

Among all system performance requirements, robust stability is a paramount condition for designs of system control. Especially in [5]-[7], numerous approaches have been proposed and these systems concerned are singularly-perturbed systems. Yahli Narkis [8] developed a relation for direct calculation of the cost function for an optimally controller linear system with quadratic criteria, disturbed by a colored noise of any given spectral density distribution. Jianguo Wang; Guangyi Cao; Jin Zhou [9] study how the optimization methods can be used to deal with plant uncertainty. A weighed sensitivity error function is presented for an optimal robust controller design in a class of stochastic model errors. As observed by the previous work that has been done for the stability, enhancing performance, and cost minimization of decentralized stochastic systems, none had focus on the robust optimal pole assignment of decentralized stochastic singularly-perturbed computer controlled systems.

In this paper, the optimal poles found are based on a reduced-order system model. The optimal pole region of the close-loop system can be realized by adjusting the state weighting matrix and the input weighting matrix. After collecting and saving all the information of the relationship among the weighting matrices and the aggregation matrix, the optimal feedback gain of the system can be understood.

2 System Prescription

The mathematical model of the n-order decentralized stochastic singularly- perturbed system is shown as:

$$\begin{cases} \dot{x} = A_{00}x + A_{01}z_1 + A_{02}z_2 + A_{03}z_3 + \dots\dots\dots A_{0m}z_m \\ \mathcal{E}\dot{z}_1 = A_{10}x + A_{11}z_1 & + B_1u_1 + G_1w_1 \\ \mathcal{E}\dot{z}_2 = A_{20}x + A_{22}z_2 & + B_2u_2 + G_2w_2 \\ \vdots & \\ \mathcal{E}\dot{z}_m = A_{m0}x & + A_{mm}z_m + B_mu_m + G_mw_m \end{cases} \quad (1a)$$

$$\begin{cases} y_1 = C_1z_1 + v_1 \\ y_2 = C_2z_2 + v_2 \\ \vdots \\ y_m = C_mz_m + v_m \end{cases} \quad (1b)$$

or
$$\dot{x} = A_{00}x + \sum_{i=1}^m A_{0i}z_i \quad (2a)$$

$$\mathcal{E}\dot{z}_i = A_{i0}x + A_{ii}z_i + B_iu_i + G_iw_i \quad (2b)$$

$$y_i = C_iz_i + v_i \quad (2c)$$

where $i=1\sim m$. The system is a linear time-invariant decentralized stochastic singularly-perturbed computer controlled system which has n-order and m independent inputs or m sub-systems. $x \in R^s$ and $z \in R^f$ are the slow and the fast state variables respectively; each sub-system z_i has its own order. $u_i \in R^{n_i}$ and $y_i \in R^{r_i}$ are the input vector of the i-th subsystem and the output vector of the i-th subsystem respectively. A_{00} , A_{0i} , A_{i0} , A_{ii} , C_i , and G_i are constant matrices with

appropriate dimensions with $i=1\sim m$. $w_i \in R^s$; w_i and v_i are disturbing noises of inputs and outputs.

3 Main Results

Finding a easy algorithm of robust sub-optimal control is the goal of this study. A system performances based on system uncertainties is necessarily investigated and tested. Uncertainties of systems are caused by the inevitable errors in system modeling due to inexact and incomplete data, simplifying approximations, neglected high frequency dynamics, and unpredicted disturbances from the environment. In this research, robust control is defined that if the desired performance still exists after using the reduced-order controllers in the full-order systems.

In this type of particular system the major uncertainty would be the fast state variables of the subsystems. Because the overall system is a decentralized computer controlled system, the responses of computer-based subsystems are a lot faster than the main plant. The responses of the fast state variables will die out pretty fast in the very initial time period. Therefore, the overall structure is potentially a singularly perturbed system. When the system reaches Quasi-steady state, the parameter ϵ can be assumed as zero. Due to this phenomenon, the fast state variables can be ignored and the order of the system can be reduced. This also rises the idea that the state model of the system can be approximated.

In Eq. (2b), the sub-station station variables, $z_1, z_2, z_3 \dots$ have reached quasi-steady state. Hence, the system order is reduced to the order of the main station which is equal to the dimension of the slow state variable x . Eq. (2b) can be shown as:

$$\begin{cases} z_1 = A_{11}^{-1}(-B_1 u_1 - A_{10} x - G_1 w_1) = -A_{11}^{-1} B_1 u_1 - A_{11}^{-1} A_{10} x - A_{11}^{-1} G_1 w_1 \\ z_2 = A_{22}^{-1}(-B_2 u_2 - A_{20} x - G_2 w_2) = -A_{22}^{-1} B_2 u_2 - A_{22}^{-1} A_{20} x - A_{22}^{-1} G_2 w_2 \\ \vdots \\ z_m = A_{mm}^{-1}(-B_m u_m - A_{m0} x - G_m w_m) = -A_{mm}^{-1} B_m u_m - A_{mm}^{-1} A_{m0} x - A_{mm}^{-1} G_m w_m \end{cases} \tag{3a}$$

Then,
$$z_i = -A_{ii}^{-1} B_i u_i - A_{ii}^{-1} A_{i0} x - A_{ii}^{-1} G_i w_i \tag{3b}$$

where $i=1\sim m$; $A_{11} \sim A_{mm}$ are nonsingular matrices. Next, recall the state equation of the slow state variable in (2a). We can obtain new representations for the equation of slow state variables by using Eq. (3b):

$$\dot{x} = [A_{00} - \sum_{i=1}^m A_{0i} A_{ii}^{-1} A_{i0}] x + \begin{bmatrix} -A_{01} A_{11}^{-1} B_1 u_1 - A_{02} A_{22}^{-1} B_2 u_2 \dots - A_{0m} A_{mm}^{-1} B_m u_m \\ u_1 \\ u_2 \\ \vdots \\ u_m \end{bmatrix} + \left[\sum_{i=1}^m -A_{0i} A_{ii}^{-1} G_i w_i \right] \tag{4}$$

Now, define $G_r = [\sum_{i=1}^m -A_{0i}A_{ii}^{-1}G_i w_i]$ and Let $G_r = Hw$ where H is a non-square

matrix and $w = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix}$. Then, $H = [\sum_{i=1}^m -A_{0i}A_{ii}^{-1}G_i w_i] w^R = [\sum_{i=1}^m -A_{0i}A_{ii}^{-1}G_i w_i]$

$[(w^T w)^{-1} w^T]$ where $w^R = [(w^T w)^{-1} w^T]$ is pseudo right inverse of w . An n-order multi-input decentralized stochastically singularly-perturbed computer controlled system is reduced into an S=(n-F)-order multi-input time-invariant system. The state model can be revised as

$$\begin{cases} \dot{x}_r = A_r x_r + B_r u + G_r = A_r x_r + B_r u + Hw & (5a) \\ y_i = C_i z_i + v_i = C_{ri} x_r + D_{ri} u_i + v_i & (5b) \end{cases}$$

where $z_i = -A_{ii}^{-1} B_i u_i - A_{ii}^{-1} A_{i0} x_r$; $C_{ri} = -C_i A_{ii}^{-1} A_{i0}$; $D_{ri} = -C_i A_{ii}^{-1} B_i$; $A_r = [A_{00} - \sum_{i=1}^m A_{0i} A_{ii}^{-1} A_{i0}]$; $B_r = [-A_{01} A_{11}^{-1} B_1 \quad -A_{02} A_{22}^{-1} B_2 \quad \dots \quad -A_{0m} A_{mm}^{-1} B_m]$;

$u = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{bmatrix}$; $G_r = [\sum_{i=1}^m -A_{0i} A_{ii}^{-1} G_i w_i]$; $w = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix}$; $i = 1, \dots, m$. Therefore, when the system

data is processed by computer, the above equations will be transformed into discrete-time model as [10]

$$x_r((k+1)h) = \Phi x_r(kh) + \Gamma u(kh) + G_r(kh) \tag{6a}$$

where $\Phi = \phi(h) = e^{A_r h}$; $\Gamma = \int_0^h \phi(\lambda) d\lambda B$. h denotes the sampling rate.

$$y_i(kh) = C_i z_i(kh) = C_{ri} x_r(kh) + D_{ri} u_i(kh) + v_i(kh) \tag{6b}$$

Now we define another non-square matrix \bar{T} , which

$$x_r = \bar{T} x_f \tag{7}$$

where the full-order state vector $x_f = \begin{bmatrix} x \\ z_i \end{bmatrix}$; $x_f \in R^{S+F}$ with $x \in R^S$ and $z \in R^F$. By

the state transformation, the non-square matrix \bar{T} that is called the fast aggregation matrix here that is used as an intermediary to have transformation between the full order model (2) and the reduced order model (5). This non-square matrix will help to shorten the derivation process.

$$A_r = \bar{T} \begin{bmatrix} A_{00} & \sum_{i=1}^m A_{0i} \\ A_{i0} / \epsilon & A_{ii} / \epsilon \end{bmatrix} \bar{T}^R = \bar{T} \begin{bmatrix} A_{00} & \sum_{i=1}^m A_{0i} \\ A_{i0} / \epsilon & A_{ii} / \epsilon \end{bmatrix} \bar{T}^T (\bar{T} \bar{T}^T)^{-1} \tag{8}$$

$$B_r = \bar{T} \begin{bmatrix} \Phi \\ B_i \end{bmatrix} \tag{9}$$

$$C_{r_i} = [\Delta \ C_i] \bar{T}^R = [\Delta \ C_i] \bar{T}^T (\bar{T} \bar{T}^T)^{-1} \tag{10}$$

where R denotes the pseudo right inverse and Δ matrix has all the elements equal to zero with appropriate size. i 's of Eq. (8) to Eq. (10) indicate the controlling subsystem. By applying Eq. (10), Eq. (8) can be revised as

$$A_r = \bar{T} \begin{bmatrix} A_{00} & \sum_{i=1}^m A_{0i} \\ A_{i0} / \varepsilon & A_{ii} / \varepsilon \end{bmatrix} [\Delta \ C_i]^L C_{r1} \tag{11}$$

Theoretically, $[\Delta \ C_i]^L$ is a singular matrix and this matrix will be crucial item to find the fast aggregation matrix, \bar{T} . Next, based on the reduced-order state model (6), Eq. (6a) can be shown as

$$x_r(k+1) = \Phi x_r(k) + \Gamma_1 u_1(k) + \Gamma_2 u_2(k) + \dots + \Gamma_m u_m(k) + G_r(kh) \tag{12}$$

where Γ_1 is the first column of Γ ; Γ_2 is the second column of Γ and so on. $u_1(k) \sim u_m(k)$ are the inputs of the subsystem one to the subsystem m . In the close-loop control systems as Fig. 1, we know

$$\begin{cases} u_1(k) = d_1(k) + K_1 x_r(k) + G_r \\ u_2(k) = d_2(k) + K_2 x_r(k) + G_r \text{ and so on.} \end{cases} \tag{13}$$

where $d_1(k)$ and $d_2(k)$ are additional inputs; G_{r1} and G_{r2} are disturbing signals.

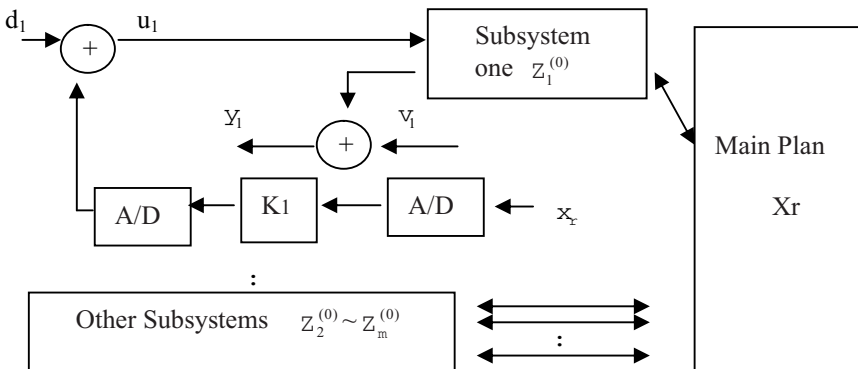


Fig. 1. The decentralized stochastic singularly-perturbed system. All the subsystems are computer processing units and assumed to be zero-order.

Now, if the main station is controlled from the subsystem one, we can assume the $d_1 \sim d_m$ and G_{r1} and G_{r2} are all disturbing noise to the controller one. They only affect the amplitude of system responses. The pole locations are unchanged.

Therefore; we revise (6) as

$$x_r(k+1) = [\Phi_N + \Gamma_1 K_1(k)]x_r(k) + JN(k) + G_r(kh) \tag{14a}$$

where $\Phi_N = (\Phi + \Gamma_2 K_2 + \Gamma_3 K_3 + \dots + \Gamma_m K_m)$ and $K_2 \sim K_m$ are existing feedback gains.

$$J = [\Gamma_1 \quad \Gamma_2 \quad \dots \quad \Gamma_m] = \Gamma; N(k) = \begin{bmatrix} d_1(k) \\ d_2(k) \\ \vdots \\ d_m(k) \end{bmatrix}$$

$$y_i(k) = C_{ri}x_r(k) + D_{ri}u_i(k) + v_i(k) \tag{14b}$$

Eq. (14) is a closed-loop state model. According to stochastic control theory [11] and singular perturbation methodology [12], the LQ performance index of each subsystem in the full order system:

$$J_i = \frac{1}{2} \sum_{k=0}^{N-1} (w^T(k)Q_i w(k) + u_i^T(k)R_i u_i(k)) \tag{15}$$

where Q_i is the weighting matrix with p. s. d. for each sub-system and

$$Q_i = \begin{bmatrix} Q_{11}^i & 0 \\ 0 & Q_{22}^i \end{bmatrix}. R_i \text{ is the weighting matrix with p. d. for each sub-system.}$$

$$w = \begin{bmatrix} x_r \\ z_i \end{bmatrix}; x_r \text{ is a slow state vector and } z_i = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} \text{ is a fast state vector.}$$

It can be presented as Eq. (16) that has the reduced order state vector, x_r .

$$J_i = \frac{1}{2} \sum_{k=0}^{N-1} (x_r^T(k)Q_{ri}x_r(k) + u_i^T(k)R_i u_i(k)) \tag{16}$$

With this constrain (16), if we have control from the subsystem one, we can have the optimal control

$$u_1^{optimal}(k) = -K_{r1}x(k) \tag{17}$$

where
$$K_{r1} = (B_{r1}^T P B_{r1} + R_1)^{-1} B_{r1}^T P \Phi_N \tag{18}$$

and, the P is the solution of the Riccati equation

$$P = \Phi_N^T \{P - P B_{r1} [B_{r1}^T P B_{r1} + R_1]^{-1} B_{r1}^T P\} \Phi_N + Q_{r1} \tag{19}$$

where P is a constant matrix. The $u_1^{optimal}$ not only minimizes the energy use but also stabilizes the system. This stabilizing feedback gain stabilizes the slow state variables of the system. There will be no control to the fast state variables; therefore, stability of

the fast state variables is required. Furthermore, in steady state, the optimal control cost from the subsystem one can also be obtained as

$$J_{\infty}^{optimal} = \frac{1}{2} x_r^T(0) P x_r(0) \tag{20}$$

The robust sub-optimal poles are

$$P_d = eig[\Phi_N + B_{r1} K_{r1}] \tag{21}$$

where P_d is the desired sub-optimal pole locations. The optimal feedback control and the optimal costs of the subsystem two to the subsystem m can be found by the same procedure used in the subsystem one. For a successful state feedback design, stabilizability is a necessary condition, and controllability is a sufficient condition.

In the forgoing process, we use the reduced order state model (6) and existing feedback gains $K_{r,2} \sim K_{r,m}$ to compute the sub-optimal feedback gain of the subsystem one: $K_{r1} = (B_{r1}^T P B_{r1} + R_1)^{-1} B_{r1}^T P \Phi_N$, if the control is performed from the subsystem one. Now, we would like to find the sub-optimal feedback gain, K_1 , for the original full order system by using the aggregation matrix, then the input of the subsystem one.

$$u_1 = -K_{r1} x_r \tag{22}$$

where x_r denotes reduced-order state. According to the state transformation technique, Eq. (22) can be shown as

$$u_1 = -K_{r1} \bar{T} x_f \tag{23}$$

$$= -K_1 x_f \tag{24}$$

where x_f denotes full-order state. By comparing with Eq. (23) and Eq. (24), we can find the relationship

$$-K_1 = -K_{r1} \bar{T} \tag{25a}$$

Also,

$$K_1 = K_{r1} \bar{T} \tag{25b}$$

where K_1 is the robust sub-optimal feedback gain implementing in the original full order system. K_{r1} is the robust sub-optimal feedback gain obtained from the reduced order system. \bar{T} is the fast aggregation matrix.

For the subsystem two to the subsystem m can follow the same method as the subsystem one to find the optimal poles by the aggregation matrix.

4 Illustrations

The whole system is a fifth-order system with three first order subsystems and three inputs. The state model is shown as

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \varepsilon \dot{z}_1 \\ \varepsilon \dot{z}_2 \\ \varepsilon \dot{z}_3 \end{bmatrix} = \begin{bmatrix} -0.5 & 0 & 0.1 & -0.2 & 0.1 \\ 0 & -1 & 0.1 & 0.3 & -0.2 \\ 0.4 & -0.3 & -0.5 & 0 & 0 \\ -0.4 & 0.4 & 0 & -0.45 & 0 \\ 0.35 & 0.3 & 0 & 0 & -0.4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ z_1 \\ z_2 \\ z_3 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.4 & 0 & 0 \\ 0 & -0.5 & 0 \\ 0 & 0 & 0.6 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} + G_i \omega_i \quad (26a)$$

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} + v_i \quad (26b)$$

where x_1 and x_2 are slow state vectors that are second-order. z_1, z_2, z_3 are all fast state vectors and first-order individually. w_i and v_i are disturbing noises of inputs and outputs. Therefore, when the system researches quasi-steady state, $\varepsilon = 0$ and the system can be reduced to a second order system such as

$$\dot{x} = \begin{bmatrix} -0.1545 & -0.163 \\ -0.363 & -0.943 \end{bmatrix} x + \begin{bmatrix} 0.08 & -0.222 & 0.15 \\ 0.08 & 0.333 & -0.3 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \quad (27)$$

Next, we digitize this reduced-order model to discrete-time domain with the sampling period 0.1.

$$x(k+1) = \begin{bmatrix} 0.985 & -0.0154 \\ -0.0344 & 0.9103 \end{bmatrix} x(k) + \begin{bmatrix} 0.0079 & -0.0223 & 0.0151 \\ 0.0075 & 0.0322 & -0.0289 \end{bmatrix} \begin{bmatrix} u_1(k) \\ u_2(k) \\ u_3(k) \end{bmatrix} \quad (28)$$

In this example, the overall state vector w is concerned with $w = \begin{bmatrix} x \\ z_i \end{bmatrix}$. Now, if we want to have the optimal control in the subsystem one, by assuming the existing $K_2 = [1 \ 1]$ and $K_3 = [5 \ 5]$, we can rewrite the model as

$$x(k+1) = \begin{bmatrix} 1.0382 & 0.0378 \\ -0.1467 & 0.7980 \end{bmatrix} x(k) + \begin{bmatrix} 0.0079 \\ 0.0075 \end{bmatrix} u_1(k) \quad (29)$$

If the performance index of the slow state vector from the subsystem one is

$$J_1 = \frac{1}{2} \sum_{k=0}^{N-1} (x^T(k) Q_1 x(k) + u_1^T(k) R_1 u_1(k)) \quad (30)$$

where $Q_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; $R_1 = 1$. The optimal control of the subsystem one:

$$u_1^{optimal} = [-3.2814 \ -0.5737] x(k) \quad (31)$$

with $P = \begin{bmatrix} 364.8580 & 61.0517 \\ 61.0517 & 13.3957 \end{bmatrix}$. The pole locations of this optimal control are 0.9820 and 0.8240; therefore, the system is stabilized by the controller, too. If the initial condition $x_r(0) = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, the optimal cost can be calculated as

$$J_1^{optimal} = \frac{1}{2} x_r^T(0) P x_r(0) \approx 500 \tag{32}$$

For the robust control test, this optimal reduced-order control will be placed back to the original full-order model. If the desired performance still exist, we have a robust control system. If $\varepsilon = 0.001$, we can have the same discrete-time model as:

$$w(k+1) = \begin{bmatrix} 0.9842 & -0.0151 & 0.0002 & -0.0004 & 0.0003 \\ -0.0334 & 0.9102 & 0.0002 & 0.0004 & -0.0005 \\ 0.8072 & -0.559 & 0 & -0.0007 & 0.0005 \\ -0.9042 & 0.8239 & 0 & 0.0001 & -0.0006 \\ 0.837 & 0.6713 & 0.0003 & 0.0001 & -0.0001 \end{bmatrix} w(k) + \begin{bmatrix} 0.0077 & 0.0218 & 0.0147 \\ 0.0074 & -0.0315 & -0.0282 \\ 0.8017 & 0.0356 & 0.0281 \\ -0.0003 & -1.1574 & -0.0373 \\ 0.012 & -0.0045 & 1.4919 \end{bmatrix} \begin{bmatrix} u_1(k) \\ u_2(k) \\ u_3(k) \end{bmatrix}$$

Now, we use the optimal feedback gain, $K_1^{optimal} = [-3.2814 \quad -0.5737]$, in the full-order system with $K_2 = [1 \quad 1]$ and $K_3 = [5 \quad 5]$. The pole locations of the system are 0.9853 and 0.8006. We can see the locations are very close to the desired pole locations; therefore, we have a robust control system.

Also, by assuming $y_1 = [0 \quad 0 \quad 1 \quad 1 \quad 1] \begin{bmatrix} x \\ z_1 \\ z_2 \\ z_3 \end{bmatrix}$, we can have the system responses

based on the subsystem one with $h=0.1$ and $\varepsilon=0.001$ as follows:

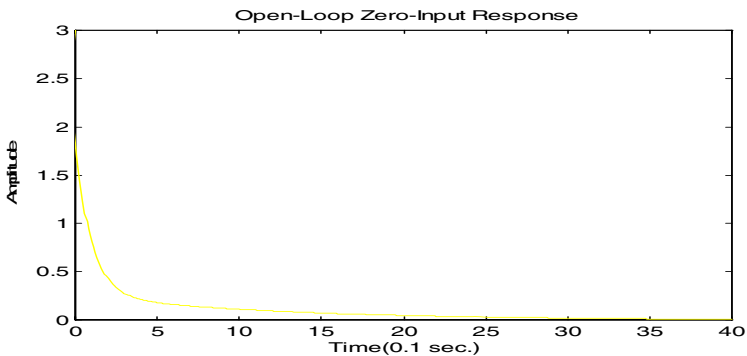


Fig. 2. The open-loop zero-input response of the full-order system with the slow state poles at 0.9915 and 0.9038

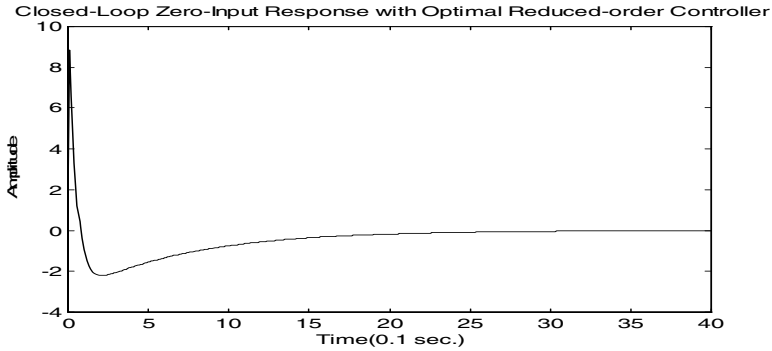


Fig. 3. The closed-loop zero-input response with the optimal reduced- order controller shifting poles to 0.9820 and 0.8240

The robustness bound of the robust control system can be found by changing the value of ε . Table 1 shows how the poles shift when the value of ε changes.

Table 1. The robust control test

| ε | Poles |
|---------------|----------------|
| 5.0000e-004 | 0.9853, 0.8008 |
| 0.0060 | 0.9853, 0.7981 |
| 0.0115 | 0.9853, 0.7951 |
| 0.0170 | 0.9854, 0.7919 |
| 0.0225 | 0.9854, 0.7883 |
| 0.0280 | 0.9854, 0.7842 |
| 0.0335 | 0.9855, 0.7795 |
| 0.0390 | 0.9855, 0.7739 |
| 0.0445 | 0.9855, 0.7673 |

In this case, if we assume the system performance allows 0.03 shift at each pole location, when $\varepsilon < 0.0115$, we can have a robust control system. The sub-optimal, reduced-order control that performs inside this bound is call robust, decentralized, sub-optimal reduced-order control. In this case, the approximated optimal poles, 0.9820 and 0.8240, are used to compare with the shifting poles caused by system uncertainties.

The robust sub-optimal control, the sub-optimal costs, and the robust control tests of the subsystem two and the subsystem three can just follow the same procedure used in the subsystem one.

After the reduced-order feedbacks are affirmed to be robust, for the full order feedback gains can be found by Eq. (8) to Eq. (10). In Eq. (9)

$$\begin{bmatrix} 0.08 & -0.222 & 0.15 \\ 0.08 & 0.333 & -0.3 \end{bmatrix} = \begin{bmatrix} t_1 & t_2 & t_3 & t_4 & t_5 \\ t_6 & t_7 & t_8 & t_9 & t_{10} \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.4 & 0 & 0 \\ 0 & -0.5 & 0 \\ 0 & 0 & 0.6 \end{bmatrix} \tag{33}$$

$$\bar{T} = \begin{bmatrix} t_1 & t_2 & 2 & 0.444 & 0.25 \\ t_6 & t_7 & 2 & 0.667 & -0.5 \end{bmatrix}$$

In Eq. (11),

$$[\Delta \ C_i]^L = ([\Delta \ C_i]^R [\Delta \ C_i])^{-1} [\Delta \ C_i]^R \cong \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Therefore;

$$\begin{bmatrix} -0.1545 & -0.163 \\ -0.363 & -0.943 \end{bmatrix} = \begin{bmatrix} t_1 & t_2 & 2 & 0.444 & 0.25 \\ t_6 & t_7 & 2 & 0.667 & -0.5 \end{bmatrix} \begin{bmatrix} -0.5 & 0 & 0.1 & -0.2 & 0.1 \\ 0 & -1 & 0.1 & 0.3 & -0.2 \\ 0.4/\varepsilon & -0.3/\varepsilon & -0.5 & 0 & 0 \\ -0.4/\varepsilon & 0.4/\varepsilon & 0 & -0.45 & 0 \\ 0.35/\varepsilon & 0.3/\varepsilon & 0 & 0 & -0.4 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0.8 & -0.6 \\ -0.889 & 0.889 \\ 0.875 & 0.75 \end{bmatrix} \tag{34}$$

The aggregation matrix is solved as $\bar{T} \cong \begin{bmatrix} 0.001 & 0.07 & 2 & 0.444 & 0.25 \\ 2 & 3.4 & 2 & 0.667 & -0.5 \end{bmatrix}$ and, the full-order feedback $K_1 = K_{r1}\bar{T} = [1.1507 \ 2.1803 \ 7.7102 \ 1.8396 \ 0.5335]$ where $K_{r1} = [-3.2814 \ -0.5737]$ found in Eq. (31). The full order feedback gains of the rest of the subsystems can follow the same procedure as above.

5 Conclusions

The full order sub-optimal feedback of the decentralized computer control of stochastic singularly-perturbed system can be found easily through the aggregation matrix and couple steps; moreover, the found robust sub-optimal reduced order feedback gain can also achieve the desired performance with decreasing cost.

By using the reduced-order state model obtained from performing the singularly methodology, the robust reduced order feedback gain can be calculated based on the slow LQ perform index. Next, the full-order feedback gain can be found by multiplying the fast aggregation matrix as Eq. (25b). The effect by applying the full order feedback and reduced order feedback will have similar performance. These two types of feedback gains provide the demand of system to adjust the control status and

performance. The completion of this algorithm helps us to analysis the decentralized computer control of stochastic singularly-perturbed system and fast to find the sub-optimal feedback gain for the full-order control and reduced-order control.

Three steps of finding the robust sub-optimal poles of the system are presented as below:

1. Find the fast aggregation matrix \bar{T} from Eq. (8)-(11).
2. Find the reduced-order sub-optimal robust feedback gain of the system from Eq. (17).
3. Find the full-order sub-optimal feedback gain of the original system from Eq. (25b).

References

1. Enea, G., Duplaix, J., Franceschi, M.: Discrete Optimal Control with Aggregation Pole Placement. IEE Proceeding-D 140(5), 309–312 (1993)
2. Arar, A., Sawan, M.E.: Design of Optimal Control Systems with Eigenvalue Placement in a Specified Region. Optimal Control Applications & Methods 16, 149–154 (1993)
3. Arar, A., Sawan, M.E.: Relation between Pole-placement and Linear Quadratic Regulator for Discrete-time Systems. J. Fanklin 334B(4), 515–523 (1997)
4. Yao, K.-c.: Computer Control of Decentralized Singularly-perturbed System. In: ICAIS 2002. First International NAISO Congress on Autonomous Intelligent Systems, Australia (2002) CD #10028-02-KY-047
5. Son, J.-W., Lim, J.-T.: Robust stability of Nonlinear Singularly Perturbed System with Uncertainties. IEE Proceedings - Control Theory and Applications 153(1), 104–110 (2006)
6. Hyun, I., Sawan, M.E., Lee, D.G., Kim, D.: Robust stability for decentralized singularly perturbed unified system. In: Proceedings of American Control Conference, pp. 4338–4343 (2006)
7. Fridman, E.: Sampled-data H_∞ Control of Linear Singularly Perturbed Systems. IEEE Transactions on Automatic Control 51(3), 470–475 (2006)
8. Narkis, Y.: Cost Function Calculation for Stationary, Linear-Quadratic System with Colored Noise. IEEE Transaction on Automatic Control 37(11), 1772–1774 (1992)
9. Wang, J., Cao, G., Zhou, J.: Optimal Robust Control for a Class of Stochastic Model Errors. In: WCICA 2006. The Sixth World Congress on Intelligent Control and Automation, vol. 1, pp. 1778–1781 (2006)
10. Astrom, K.J., Wittenmark, B.: Computer-controlled Systems: Theory and Design. Prentice-Hall Inc., NJ (1997)
11. Stengel, R.: Stochastic Optimal Control. John Wiley & Sons, NY (1986)
12. Naidu, D.S.: Singular Perturbation Methodology in Control Systems. Peter Peregrinus Ltd., London (1988)

Assured-Timeliness Integrity Protocols for Distributable Real-Time Threads with in Dynamic Distributed Systems

Binoy Ravindran¹, Edward Curley¹, Jonathan S. Anderson¹,
and E. Douglas Jensen²

¹ Department of Electrical and Computer Engineering
Virginia Tech, Blacksburg Virginia, 24061, USA
{binoy, alias, andersoj}@vt.edu

² The MITRE Corporation
Bedford, Massachusetts, 01730, USA
jensen@mitre.org

Abstract. Networked embedded systems present challenges for designers composing distributed applications with dynamic, real-time, and resilience requirements. We consider the problem of recovering from failures of distributable threads with assured timeliness in dynamic systems with overloads, and node and (permanent/transient) network failures. When a failure prevents timely execution, the thread must be terminated, requiring detecting and aborting thread orphans and delivering exceptions to the farthest, contiguous surviving thread segment for possible resumption, while optimizing system-wide timeliness. A scheduling algorithm (HUA) and two thread integrity protocols (D-TPR and W-TPR) are presented and shown to bound orphan cleanup and recovery times with bounded loss of best-effort behavior. Implementation experience using the emerging Distributed Real-Time Specification for Java (DRTSJ) demonstrates the algorithm/protocols' effectiveness.

1 Introduction

In distributed systems, action and information timeliness is often end-to-end—e.g., a causally dependent, multi-node, sensor to shooter sequential flow of execution in network-centric warfare systems [1]. Designers and users of distributed systems often need to dependably reason about (specify, manage, predict) end-to-end timeliness. Many emerging such systems are being envisioned to be built using ad hoc network systems—e.g., those without a fixed infrastructure, having dynamic node membership and network topology changes, including mobile, ad hoc wireless networks [2].

Maintaining end-to-end properties (e.g., timeliness, connectivity) of a control or information flow requires a model of the flow's locus in space and time that can be reasoned about. Such a model facilitates reasoning about, and resolving the contention for resources that occur along the flow's locus. The *distributable thread* abstraction which first appeared in the Alpha OS [3] and later

in MK7.3 [4], OMG’s Real-Time CORBA 1.2 [5], and Sun’s emerging Distributed Real-Time Specification for Java (DRTSJ) [6] provide such a model as first-class programming and scheduling abstractions. A distributable thread (see Figure 1) is a thread of execution with a globally unique identity that extends and retracts through local and remote objects, carrying its execution context (e.g., scheduling parameters) as it transits node boundaries [5]. This context is used in resolving resource contention among threads with the objective of maximizing a particular scheduling objective. We focus on distributable threads (hereafter, simply *threads*) as our end-to-end control flow/scheduling abstraction.

During overload it is impossible to meet time constraints for all threads: the demand exceeds the supply. A distinction must be made between urgency and importance in order to select which activities to execute and when (During underloads, such a distinction generally need not be made—e.g., if all time constraints are deadlines, then EDF [7] can meet all deadlines, and no selection must be made.) Traditional deadlines do not capture this distinction, thus we consider the *time/utility function* (or TUF) model [8] that specifies the utility of completing a thread as a function of its completion time. In this paper, we specify a deadline as a binary-valued, downward “step” shaped TUF. A thread’s TUF decouples its importance (X-axis) and urgency (Y-axis).

When thread time constraints are expressed with TUFs, the scheduling optimality criteria are based on maximizing accrued utility—e.g., maximizing the total thread accrued utility. Such criteria are called *utility accrual* (or UA) criteria, and sequencing (scheduling, dispatching) algorithms that optimize UA criteria are called UA sequencing algorithms (e.g., [9,10]).

Our Contributions. When nodes fail, threads may be divided into several pieces. Segments of a thread that are disconnected from its node of origin (called the thread’s *root*), are called *orphans*. When threads fail and cause orphans, application-supplied exception handlers must be released for execution on the orphan nodes. Such handlers may have time constraints themselves and will compete for their nodes’ processor along with other threads. Under a termination model, when handlers execute (not necessarily when they are released), they will abort the associated orphans after performing recovery actions that are necessary to avoid inconsistencies. Once all handlers complete, thread execution can potentially be resumed from the farthest, contiguous surviving thread segment (from the thread’s root). Such a coordinated set of recovery actions will preserve the abstraction of a continuous reliable thread.

A straightforward approach for scheduling handlers is to model them as traditional (single-node) threads. Further, the classical *admission control* strategy

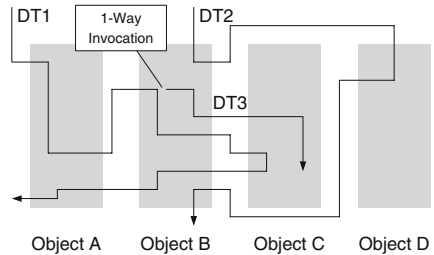


Fig. 1. Distributable Threads

[11, 12, 13] can be used: When a thread T arrives on a node, if a feasible node schedule can be constructed such that it includes all the previously admitted threads and their handlers, besides T and its handler, then admit T and its handler; otherwise, reject. But this will cause the very fundamental problem that is solved by UA schedulers through their best-effort decision making—i.e., a newly arriving thread is rejected because it is infeasible, despite that thread being the most important. In contrast, UA schedulers will feasibly complete the high importance newly arriving thread (with high likelihood), at the expense of not completing some previously arrived ones, since they are now less important than the newly arrived.

In this paper, we consider the problem of recovering from thread failures with assured timeliness and best-effort property. We consider distributable threads that are subject to TUF time constraints. Threads may have arbitrary arrival behaviors, may exhibit unbounded execution time behaviors (causing node overloads), and may span nodes that are subject to arbitrary crash failures and a network with permanent/transient failures and unreliable transport mechanisms. Another distinguishing feature of motivating applications for this model (e.g., [1]) is their relatively long thread execution time magnitudes—e.g., milliseconds to minutes. For such a model, we consider the scheduling objective of maximizing the total thread accrued utility.

We present a UA scheduling algorithm called *Handler-assured Utility Accrual scheduling algorithm* (or HUA) for thread scheduling, and two protocols called *Decentralized Thread Polling with bounded Recovery* (or D-TPR) and *Wireless Thread Polling with bounded Recovery* (or W-TPR) for ensuring thread integrity. D-TPR targets networks with generally permanent network failures, and W-TPR targets mobile, ad hoc wireless networks with generally transient network failures. We show that HUA and D-TPR/W-TPR ensure that handlers of threads that encounter failures during their execution will complete within a bounded time, yielding bounded thread cleanup time. Yet, the algorithm/protocols retain the fundamental best-effort property of UA algorithms with bounded loss—i.e., a high importance thread that may arrive at any time has a very high likelihood for feasible completion. Our implementation experience using DRTSJ's emerging Reference Implementation (RI) demonstrates the algorithm/protocols' effectiveness.

Thread integrity protocols have been developed in the past—e.g., Thread Polling with Recovery [13], Alpha's Thread Polling [3], Node Alive protocol [14]. None of these efforts provide time-bounded thread cleanup in the presence of node and (permanent/transient) network failures and unreliable transport mechanisms. Further, [13] suffers from unbounded loss of the best-effort property due to its admission control strategy (we show this in Section 3.3). In contrast, HUA and D-TPR/W-TPR provide bounded thread cleanup with bounded loss of the best-effort property in the presence of (permanent/transient) network failures and unreliable transport mechanisms — the first such algorithm/protocols. Thus, the paper's contribution is the HUA and D-TPR/W-TPR.

2 Models and Objectives

Threads. Threads execute in local and remote objects by location-independent invocations and returns. The portion of a thread executing an object operation is called a *thread segment*; a thread can be viewed as being composed of a series of thread segments. A thread's initial segment is called its *root* and its most recent segment is called its *head*, the only segment that is active. A thread can also be viewed as being composed of a sequence of *sections*, where a section is a maximal length sequence of contiguous thread segments on a node.

A section's execution time estimate is known when the thread arrives at the section's node. This execution time estimate includes that of the section's normal code and its exception handler code, and can be violated at run-time (e.g., due to context dependence, causing processor overloads). However, the number of thread sections is unknown *a priori*. The application is comprised of a set of threads, denoted $\mathbf{T} = \{T_1, T_2, T_3, \dots\}$.

Timeliness Model. Each thread T_i 's time constraint is specified using a TUF, denoted $U_i(t)$. Downward step TUFs generalize classical deadlines where $U_i(t) = \{0, \{n\}\}$. We focus on *non-increasing* (unimodal) TUFs, as they encompass the majority of time constraints of interest to us (e.g., [15]).

Each TUF U_i has an initial time I_i , which is the earliest time for which the function is defined, and a termination time X_i , which denotes the last point that the function crosses the X-axis.

Abort Model. Each section of a thread has an associated exception handler. We consider a termination model for all thread failures. If a thread has not completed by its termination time, or a thread encounters a network or node failure, an exception is raised, and handlers are released on all nodes hosting thread's sections. When a handler executes, it will abort the associated section after performing recovery actions that are necessary to avoid inconsistencies—e.g., rolling back/forward section's held logical and physical resources to safe states.

Each handler may also have a TUF time constraint, and an execution time estimate, provided by the handler's thread when the thread arrives at a node. Violation of the termination time of a handler's TUF will cause the immediate execution of system recovery code on that node, which will recover the thread section's held resources and return the system to a consistent and safe state.

System and Failure Models. We consider a system model where a set of processing *nodes* $N_i \in N, i \in [1, m]$ are interconnected via a network. We consider an unreliable multihop network model (e.g., WAN, MANET), with nodes interconnected through routers. Node clocks are synchronized—e.g., using [16]. Nodes may fail arbitrarily by crashing (i.e., fail-stop), while network links may fail transiently or permanently, causing network partitions.

We consider Real-Time CORBA 1.2's [5] *Case 2* approach for thread scheduling. According to this approach, node schedulers use thread scheduling parameters and independently schedule thread sections to optimize the system-wide timeliness optimality criteria, resulting in approximate, global, system-wide timeliness.

Scheduling Objectives. Our primary objective is to maximize the total thread accrued utility as much as possible. Further, the orphan cleanup and recovery time must be bounded, while retaining the best-effort property of UA algorithms.

3 The HUA Algorithm

3.1 Rationale

Section Scheduling. Since the task model is dynamic—i.e., when threads will arrive at nodes, and how many sections a thread will have are statically unknown, node (section) schedules must be constructed solely exploiting the current system knowledge. A reasonable heuristic is a “greedy” strategy at each node: Favor “high return” thread sections over low return ones, and complete as many of them as possible before thread termination times, as early as possible.

The potential utility that can be accrued by executing a thread section on a node defines a measure of that section’s “return on investment.” We measure this using a metric called the *Potential Utility Density* (or PUD) [10]. On a node, a section’s PUD measures the utility that can be accrued by immediately executing it on the node, per unit of remaining execution time.

However, a section may encounter failures. We first define the concept of a *section failure* and a *released handler*:

Definition 1 (Section Failure). Consider a section S_i of a thread T_i . We say that S_i has failed when (a) S_i violates the termination time of T_i while executing, thereby raising a time constraint-violation exception on S_i ’s node; or (b) a failure-exception notification is received at S_i ’s node regarding the failure of a section of T_i that is upstream or downstream of S_i , which designates S_i as an “orphan-head.”

Definition 2 (Released Handler). A handler is released for execution when its section fails according to Definition 1.

In the absence of section failure the corresponding section PUD can be obtained as the utility accrued by executing the section divided by the time spent for executing the section. The section PUD for a failure scenario (per Definition 1) can be obtained as the utility accrued by executing the handler of the section divided by the total time spent for executing the section and the handler.

Thus, on each node, HUA examines thread sections for potential inclusion in a feasible node schedule in the order of decreasing section PUD. For each section, the algorithm examines whether that section and its handler can be feasibly completed, in which case it is added to the schedule.

If a non-head section S_i is not included, it is conceptually equivalent to the (crash) failure of N_i . This is because, S_i ’s thread T_i has made a downstream invocation after arriving at N_i and is yet to return from that invocation. If T_i had made a downstream invocation, then S_i had executed before, and hence was feasible and had a feasible handler at that time. S_i ’s rejection now invalidates that previous feasibility. Thus, S_i must be reported as failed and a thread break

for T_i at N_i must be reported to have occurred to ensure system-wide consistency on thread feasibility. The algorithm does this by interacting with the integrity protocol (e.g., D-TPR).

This process ensures that included sections always have feasible handlers. Further, all upstream sections' handlers are also feasible. When any such section fails, its handler and all upstream handlers will complete in bounded time.

No such assurances are afforded to sections that fail otherwise—i.e., the termination time expires for S_i , which has not completed its execution and is not executing when the expiration occurs. Thus, S_i and its handler are not part of the feasible schedule at the expiration time. S_i 's handler is executed in a best-effort manner, in accordance with its potential contribution to the total utility.

Feasibility. Feasibility of a section on a node can be tested by verifying whether the section can be completed on the node before the section's distributable thread's end-to-end termination time. Using a thread's end-to-end termination time for verifying the feasibility of a section of the thread may potentially overestimate the section's slack, especially if there are a significant number of sections that follow it in the thread. However, this is a reasonable choice, since the number of sections of a thread is unknown (otherwise approaches from [17] apply).

A handler is feasible if it can complete before its *absolute* termination time. Failure time is impossible to predict, so a reasonable choice for the handler's absolute termination time is the thread's end-to-end termination time, plus the handler's termination time, delaying the handler's latest start time.

3.2 Algorithm Overview

HUA's scheduling events at a node include the arrival of a thread at the node, release of a handler at the node, completion of a thread section or a section handler at the node, and the expiration of a TUF termination time at the node. To describe HUA, we introduce a number of variables and auxiliary functions which are largely self-explanatory. Detailed descriptions appear in the full version of this paper.

HUA is shown in Algorithm 1. Invoked at time t_{cur} , HUA H and checks the feasibility of the sections. If a section's earliest predicted completion time exceeds its termination time, it is not included. Otherwise, HUA calculates its PUD. Sections are then sorted by PUD (line 8), and those with positive PUD are iteratively inserted into σ , maintained in the non-decreasing order of section termination times. Thus, a section S_i and S_i^h are inserted into σ at positions that correspond to $S_i.X$ and $S_i.X + S_i^h.X$, respectively.

If after inserting S_i and S_i^h into σ , σ becomes infeasible, S_i and S_i^h are removed. If a section S_i that is removed is not a head and belonged to the previous schedule, the integrity protocol is notified regarding S_i 's failure. If one or more handlers have been released but have not completed their execution, the algorithm checks whether any of those handlers are missing in σ . If any handler is missing, the handler at the head of H is selected for execution. If all handlers in H have been included in σ , the section at the head of σ is selected.

Algorithm 1. HUA: High Level Description

```

1: input:  $S_r, \sigma_r, H$ ; output: selected thread  $S_{exe}$ ;
2: Initialization:  $t := t_{cur}$ ;  $\sigma := \emptyset$ ;  $HandlerIsMissed := \text{false}$ ;
3: updateReleaseHandlerSet ();
4: for each section  $S_i \in S_r$  do
5:   if  $feasible(S_i) = \text{false}$  then
6:     reject( $S_i$ );
7:   else  $S_i.PUD = \min\left(\frac{U_i(t+S_i.ExT)}{S_i.ExT}, \frac{U_i^h(t+S_i.ExT+S_i^h.ExT)}{S_i.ExT+S_i^h.ExT}\right)$ 
8:  $\sigma_{tmp} := \text{sortByPUD}(S_r)$ ;
9: for each section  $S_i \in \sigma_{tmp}$  from head to tail do
10:  if  $S_i.PUD > 0$  then
11:    Insert( $S_i, \sigma, S_i.X$ );
12:    Insert( $S_i^h, \sigma, S_i.X + S_i^h.X$ );
13:    if  $feasible(\sigma) = \text{false}$  then
14:      Remove( $S_i, \sigma, S_i.X$ );
15:      Remove( $S_i^h, \sigma, S_i.X + S_i^h.X$ );
16:      if  $IsHead(S_i) = \text{false}$  and  $S_i \in \sigma_r$  then
17:        alertProtocol( $S_i$ );
18:    else break;
19: if  $H \neq \emptyset$  then
20:   for each section  $S^h \in H$  do
21:    if  $S^h \notin \sigma$  then
22:      $HandlerIsMissed := \text{true}$ ;
23:     break;
24: if  $HandlerIsMissed := \text{true}$  then
25:   $S_{exe} := \text{headOf}(H)$ ;
26: else
27:   $\sigma_r := \sigma$ ;
28:   $T_{exe} := \text{headOf}(\sigma)$ ;
29: return  $S_{exe}$ ;

```

3.3 Algorithm Properties

Theorem 1. *If a section S_i fails (per Definition 1), then under HUA with zero overhead, its handler S_i^h will complete no later than $S_i.X + S_i^h.X$ (barring S_i^h 's failure).¹*

Consider a thread T_i that arrives at a node and releases a section S_i after the handler of a section S_j has been released on the node (per Definition 2) and before that handler (S_j^h) completes. Now, HUA may exclude S_i from a schedule until S_j^h completes, resulting in some loss of the best-effort property. To quantify this loss, we define the concept of a *Non Best-effort time Interval* (or NBI):

Definition 3. *Consider a scheduling algorithm \mathcal{A} . Let a section S_i arrive at a time t with the following properties: (a) S_i and its handler together with all sections in \mathcal{A} 's schedule at time t are not feasible at t , but S_i and its handler are feasible just by themselves; (b) One or more handlers (which were released before t) have not completed their execution at t ; and (c) S_i has the highest PUD among all sections in \mathcal{A} 's schedule at time t . Now, \mathcal{A} 's NBI, $NBI_{\mathcal{A}}$, is defined*

¹ Proofs of all theorems have been eliminated for space, but are available in the full version of this paper at <http://www.real-time.ece.vt.edu/eso07.pdf>

as the duration of time that S_i will have to wait after t , before it is included in \mathcal{A} 's feasible schedule. Thus, S_i is assumed to be feasible together with its handler at $t + NBI_{\mathcal{A}}$.

We now describe the NBI of HUA and other UA algorithms including DASA [10], LBESA [9], and AUA [13] (under zero overhead):

Theorem 2. *HUA's worst-case NBI is $t + \max_{S_j \in \sigma_t} (S_j.X + S_j^h.X)$, where σ_t is HUA's schedule at time t . DASA's and LBESA's worst-case NBI is zero; AUA's is $+\infty$.*

Theorem 3. *Best-case NBI of HUA, DASA, and LBESA is 0; AUA's is $+\infty$.*

4 The D-TPR Protocol

D-TPR targets systems with node and network failures that are generally permanent. The protocol is instantiated in a per-node component called the Thread Integrity Manager (or TIM), which continually runs D-TPR's polling operation. TIM operations are considered to be administrative operations, and they are conducted with scheduling eligibility exceeding all application threads. We thus ignore the (comparatively small, and bounded) processing delays on each node in the analysis.

4.1 Polling

At every polling interval t_p , the TIM on each node identifies locally-hosted sections, sending a POLL message to each of its predecessor and successor nodes for each section. Each POLL message containing corresponding local and remote section IDs for each section. If the entry type is SUCCESSOR, the remote section ID will correspond to the successor section of the local section in the entry. Similarly, the remote section ID of PREDECESSOR corresponds to the predecessor section of the local segment in the entry. In this way, the node receiving the POLL message is able to discern (downstream or upstream) the message's origin and thus from which direction the section has been deemed healthy.

4.2 Break Detection

When an invocation is made, D-TPR creates timers which are set to a delay D , the likely worst-case message delay incurred in the network, and is empirically determined (similar to our measurements in Section 6). One timer is established for the downstream section and the other is established for the upstream section. The TIM on the node making the invocation (upstream side) creates a downstream-invocation timer that will cause a timeout when polling messages have not been received from downstream frequently enough. The TIM on the node hosting the remote object to which the invocation is being made (downstream side) creates an upstream-invocation timer that will cause a timeout when polling messages are not received from upstream frequently enough.

When a POLL message is received from upstream, the upstream-invocation timer is reset to D and resumes counting down. The same is true of the downstream-invocation timer when a POLL message is received from downstream. A “thread break” is declared when either the upstream or downstream-invocation time reaches zero.

Lemma 4. *Consider a section S_i and its successor section S_j . Under D-TPR, if S_j 's node fails, or S_i becomes unreachable from S_j (but not necessarily vice versa), then S_i will detect a thread break between S_i and S_j within $t_p + D$.*

Lemma 5. *Consider a section S_j and its predecessor S_i . Under D-TPR, if S_i 's node fails, or S_j becomes unreachable from S_i (but not necessarily vice versa), then S_j will detect a thread break between S_i and S_j within $t_p + D$. S_j and its downstream sections are now said to be orphaned.*

4.3 Recovery

Recovery operations are administrative functions carried on below the level of application scheduling. While recovery proceeds, D-TPR activities continue concurrently, allowing the protocol to recognize and deal with multiple simultaneous breaks and cleanup operations.

If the upstream-invocation timer expires, the protocol assumes that the upstream section is unreachable and declares the local section associated with the timer to be an *orphan*. D-TPR then attempts to force the upstream section to become the thread's *new head* while forcing the downstream section to become an *orphan*. To force the upstream section to become the *new head*, the protocol sends a NEW_HEAD message upstream and stops upstream POLL messages, which refresh the upstream section. If the upstream node receives the NEW_HEAD message, the upstream section will immediately begin behaving like a *new head*. If the upstream node does not receive the message, the upstream section's downstream-invocation timer will expire (due to the stopped POLL messages) forcing the section to become the *new head*.

In order to force the downstream section to become an *orphan*, the protocol sends an ORPHANPROP message downstream and modifies its downstream POLL messages to include an orphan status. The downstream node will either receive the ORPHANPROP message and become an *orphan*, or the downstream section's timer will expire forcing it to become an *orphan*. When a section becomes an orphan, it propagates the ORPHANPROP message in order to identify all orphans.

When a section's downstream-invocation timer expires, the protocol assumes that the downstream sections are unreachable and declares itself the *new head* of the thread. The *new head* then sends an ENDORPHAN downstream and ceases downstream refresh polling. In this way, the downstream section will either receive the ENDORPHAN notification and become an *orphan* or its upstream timer will expire, making the section an orphan.

Lemma 6. *Under D-TPR, if a thread break occurs between S_i and its successor S_j , then S_i will become the new head within $t_p + 2D$. Since the new head of*

a thread is always directly upstream from a break, D-TPR therefore activates a new head within $t_p + 2D$.

Lemma 7. Under D-TPR, if a thread break occurs between S_i and its successor S_j , then S_j will identify itself as an orphan within $t_p + 2D$.

4.4 Cleanup

An orphaned section releases its exception handler only if it is an “orphan-head.” This can happen in one of three ways: (1) The current head of the thread becomes an orphan; (2) A non-head orphan is returned to by an orphan-head and becomes a new orphan-head; and (3) An orphan’s downstream-invocation timer expires forcing it to become a new orphan-head.

Theorem 8. Under D-TPR/HUA, if a thread break occurs between a section S_i and its successor S_j , then all orphans from S_j till the thread’s current head S_{j+k} , for some $k \geq 1$, will be aborted in the LIFO-order—i.e., from S_{j+k} to S_j —and will complete by $t_p + (2 + k)D + \sigma_{\alpha=0}^k(S_{j+\alpha}.X + S_{j+\alpha}^h.X)$, unless a section $S_{j+\alpha}$ becomes unreachable from $S_{j+\alpha+1}, 0 \leq \alpha \leq k - 1$.

Theorem 9. Under D-TPR/HUA, if a thread breaks, then the thread’s orphans will complete within a bounded time.

5 The W-TPR Protocol

W-TPR is designed for mobile, ad hoc wireless networks, where communication is assumed to be unreliable and prone to transient failures. The protocol exploits the fact that a thread is only adversely affected by a thread break if the head attempts to move across that break. In contrast, D-TPR detects a break and assumes that the break will be permanent; so it preempts the possibility of the head crossing the break by eliminating sections beyond the break point. W-TPR assumes that the breaks are not permanent.

W-TPR differs from D-TPR primarily in the way thread-breaks are determined. In W-TPR, breaks are never actually recognized. Instead, the protocol recognizes when communication errors affect either an invocation or a return (head movement) and provides maintenance accordingly.

Figure 2 shows the section states and transitions in W-TPR. No breaks are ever declared—a section becomes an orphan only if it receives the ORPHAN message from an upstream section. Sections are healthy until notified otherwise.

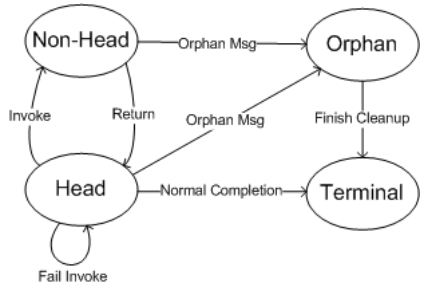


Fig. 2. Section State Diagram

Downstream Head Movement. During an invocation, a thread section S_i makes a call on a remote object, which creates a second section S_{i+1} . In order for the invocation to be successful, S_{i+1} must be created and S_i is made aware of S_{i+1} .

An invocation request is sent downstream and the local section, S_i , begins waiting for invocation verification. The invocation is verified when the local section receives an INV-ACK from the downstream node or a POLL from the downstream node containing the section ID of the remote section (see further).

When the invocation is received by the downstream node, the downstream node attempts to finalize the invocation and sends an INV-ACK message to the upstream section. The downstream node begins sending periodic POLL messages to the upstream section, at every polling interval t_p . When a healthy section receives a POLL message from an *orphan*, the healthy section returns an ORPHAN message to the *orphan*. If the *orphan* is not the *orphan-head*, similar to D-TPR, the ORPHAN message is propagated upstream.

The protocol resends the invocation request until either the invocation is verified, or the protocol deems that communication with the downstream node is not possible by waiting for an application-specified value t_n to expire and no INV-ACK or a POLL message is received from the downstream node during t_n . If communication with the downstream node is not possible, then the local section maintains head status and the application is notified that the invocation has failed. The TIM also sends an ORPHAN message downstream, in the event that only a partial invocation was accomplished. Thus the downstream node's INV-ACK/POLL messages are not received upstream while thread execution progresses on the downstream node and further downstream.

Lemma 10. *Under W-TPR thread head location is ambiguous for at most t_n .*

Upstream Head Movement. When the head is moving from the local node to an upstream node, the local node begins waiting for return verification from the upstream node. When the return message is received by the upstream node, the upstream node sends a return verification message RETURN-ACK downstream to the local node. If the verification is not received within t_n , then the return times out and the protocol forces the return message to be resent, which chains upstream. Even in the presence of upstream communication errors, the downstream section never becomes an *orphan*. Since the section has already finished executing and has a healthy return value, it is fruitless to abort this section before delivering its return value.

Lemma 11. *Under W-TPR, a thread's head is never disconnected from the rest of the thread and no new head activation is required.*

Cleanup. A section becomes an *orphan* upon receipt of an ORPHAN message, in response to its POLL. When the ORPHAN message is received, the section propagates that message downstream and waits for a return from its downstream section to be designated an orphan-head before starting cleanup, as in D-TPR. Cleanup begins when the furthest orphaned section is notified it is an orphan.

Theorem 12. *Under W-TPR, if a section S_i makes an unsuccessful invocation to its (potential) successor section S_j (i.e., S_j will be S_i 's successor had if the invocation was successful), then all orphans that can potentially be created from S_j till the thread's furthest orphaned section $S_{j+k}, k \geq 1$, will be aborted in the LIFO-order and will complete within a bounded time under HUA, as long as no further failures occur between S_j and S_{j+k} .*

Theorem 12 holds only if no further failures occur between S_j and S_{j+k} . D-TPR can detect such failures due to its continuous pairwise polling operation, whereas W-TPR is unable to do so precisely due its "on-demand" polling.

6 Implementation Experience

HUA, D-TPR, and W-TPR were implemented in DRTSJ's RI [6]. The RI includes a threads API, user-space scheduling framework for pluggable thread scheduling, and mechanisms for implementing thread integrity protocols, running atop Apogee's Real-Time Specification for Java (RTSJ)-compliant Apheleon Java Virtual Machine. The experiments and RI ran on the Debian Linux OS (kernel version 2.6.16-2-686) on 800MHz Pentium-III machines.

Metrics of interest included total thread cleanup time and protocol overhead as measured by thread completion time. We measured these during 100 experimental runs of our test application. Each experimental run spawned a single distributable thread which propagated to five other nodes, returning back through the same five nodes.

Total cleanup time is the time between the failure of a thread's node or communication link and the completion of the handlers of all the orphan sections of the thread. Figures 3(a) and 3(b) show the measured cleanup times for HUA/D-TPR and HUA/W-TPR, respectively. The cleanup times are plotted against the protocols' cleanup upper bound times for the thread set used in our experiments. We observe that both HUA/D-TPR and HUA/W-TPR satisfy their cleanup upper bound, validating Theorem 9.

Completion time is the difference between when a root section starts execution and when it completes. Figures 4(a) and 4 show the thread completion times of experiments 1) with failures and D-TPR/W-TPR, 2) without failures but with D-TPR/W-TPR, 3) without failures and without D-TPR/W-TPR, and 4) with failures but without D-TPR/W-TPR. We measure the overhead each protocol incurs in terms of the increase in thread completion times.

Figure 4(a) shows the completion times for experiments with and without D-TPR. We observe that the completion times of successful threads without D-TPR is smaller than that with D-TPR. This is to be expected as D-TPR incurs a non-zero overhead. However, we also observe that the completion times of failed threads with D-TPR are shorter than even the completion times of successful threads without D-TPR. This is because, orphan cleanup can occur in parallel with the continuation of a repaired thread, allowing the repaired thread to finish without waiting for all orphans to run to completion. A successful thread, on the other hand, must wait for all sections to finish before it can complete, increasing

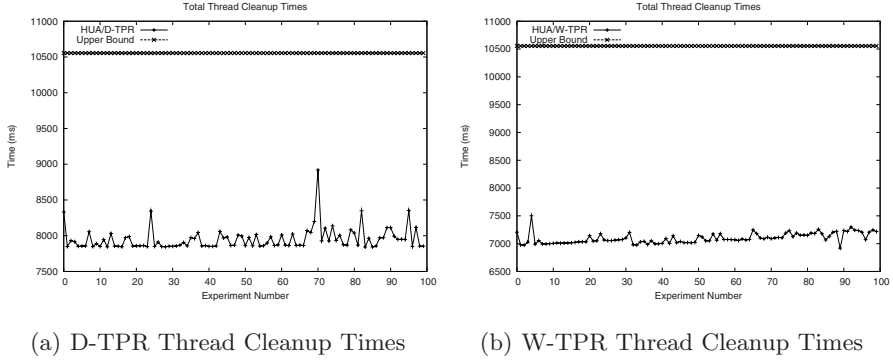


Fig. 3. Thread Cleanup Times for D-TPR and W-TPR

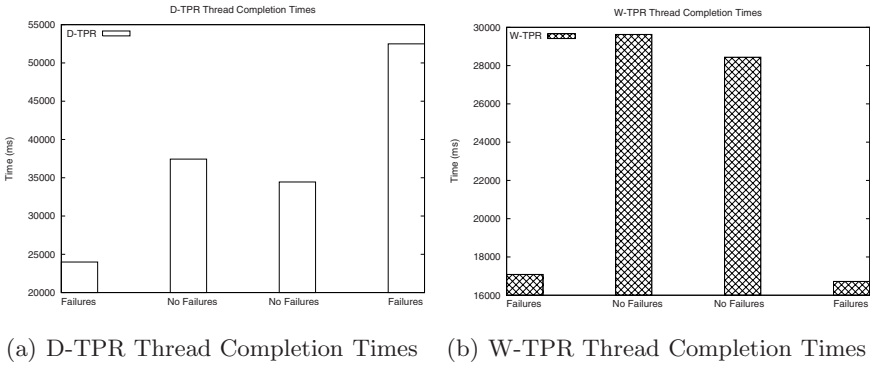


Fig. 4. W-TPR Thread Completion Times

its completion time. Figure 4(a) also shows that failed threads with D-TPR complete much more quickly than failed threads with no D-TPR support.

Figure 4 shows completion times for experiments run with and without W-TPR. As the figure shows, the measurements taken in the absence of W-TPR are only slightly lower than the measurements taken in the presence of W-TPR. We observe that W-TPR incurs relatively little overhead while providing the properties discussed in Section 5.

7 Conclusions and Future Work

We present a real-time scheduling algorithm called HUA and two protocols called D-TPR and W-TPR. We show that HUA and D-TPR/W-TPR bound the orphan cleanup and recovery time with bounded loss of the best-effort property — the first such algorithm/protocols for systems with (permanent/transient)

network failures and unreliable transport. Our implementation using the emerging DRTSJ/RI demonstrates the algorithm/protocols' effectiveness.

Directions for future work include allowing threads to share non-CPU resources, establishing assurances on thread time constraint satisfactions', and extending results to arbitrary graph-shaped, multi-node, causal control/data flows.

References

1. CCRP: Network centric warfare, <http://www.dodccrp.org/ncwPages/ncwPage.html>
2. Baker, F.: An outsider's view of manet. Internet-Draft, Work. In Progress draft-baker-manet-review-01.txt, IETF Network Working Group (March 2002)
3. Northcutt, J.D.: Mechanisms for Reliable Distributed Real-Time Operating Systems — The Alpha Kernel. Academic Press, London (1987)
4. The Open Group: MK7.3a Release Notes. The Open Group Research Institute, Cambridge, Massachusetts (1998)
5. OMG: Real-time corba 2.0: Dynamic scheduling specification. Technical report, Object Management Group (2001)
6. Anderson, J., Jensen, E.D.: The distributed real-time specification for java: Status report. JTRES (2006)
7. Horn, W.: Some simple scheduling algorithms. Naval Research Logistics Quaterly 21, 177–185 (1974)
8. Jensen, E.D., et al.: A time-driven scheduling model for real-time systems. In: IEEE RTSS, pp. 112–122 (December 1985)
9. Locke, C.D.: Best-Effort Decision Making for Real-Time Scheduling. PhD thesis, CMU, CMU-CS-86-134 (1986)
10. Clark, R.K.: Scheduling Dependent Real-Time Activities. PhD thesis, CMU, CMU-CS-90-155 (1990)
11. Nagy, S., Bestavros, A.: Admission control for soft-transactions in accord. In: IEEE RTAS, p. 160 (1997)
12. Streich, H.: Taskpair-scheduling: An approach for dynamic real-time systems. Mini & Microcomputers 17(2), 77–83 (1995)
13. Curley, E., et al.: Recovering from distributable thread failures with assured timeliness in real-time distributed systems. In: IEEE SRDS, pp. 267–276 (2006)
14. Goldberg, J., et al.: Adaptive fault-resistant systems (chapter 5: Adaptive distributed thread integrity). Technical Report csl-95-02, SRI International (1995)
15. Clark, R., et al.: An adaptive, distributed airborne tracking system. In: IEEE WPDRTS, pp. 353–362 (1999)
16. Romer, K.: Time synchronization in ad hoc networks. In: ACM MobiHoc, pp. 173–182 (2001)
17. Kao, B., et al.: Deadline assignment in a distributed soft real-time system. IEEE TPDS 8(12), 1268–1274 (1997)

Evaluating Modeling Solutions on Their Ability to Support the Partitioning of Automotive Embedded Systems

Augustin Kebemou¹ and Ina Schieferdecker²

¹ Fraunhofer Institute for
Software and Systems Engineering (ISST)
Mollstrasse 1, 10178 Berlin, Germany

² Fraunhofer Institute for
Open Communication Systems (FOKUS)
Kaiserin-Augusta-Allee 31, 10589 Berlin, Germany

Abstract. A pool of competing modeling solutions have been proposed to cope with the problems induced by the growing complexity of automotive embedded systems, i.e. the E/E (Electric/Electronic) systems of automobiles. As the principal features of these solutions are axed around modularization and high level of abstraction, it is necessary to investigate their ability to support the implementation. An objective evaluation will be helpful to define how each modeling technique should be enhanced for a better support of the implementation, whenever necessary. This paper defines a framework to evaluate the capacity of modeling techniques to support the implementation in the automotive engineering domain, particularly the partitioning. Following the state-of-the-art in the partitioning of automotive embedded systems, we present the evaluation framework. Then, we introduce the most common modeling solutions used in the automotive embedded systems design and we use the framework to evaluate and classify them.

Index Terms: Automotive, embedded systems, modeling, partitioning.

1 Introduction

The development of Automotive Embedded Systems (AES) has incontestably experienced a great leap forward during the last decade. On the way to its maturity, the AES design has adopted the model-based development scheme. Model-based development offers an effective way to decrease the technical and financial risk of "try and error" and improves the economy (design time, material usage, etc.) and the quality (reliability, soundness, performance, EMC, etc.) of the system. Furthermore, model-based development has the potentiality to boost the innovation, afford collegiate work and simplify the product maintenance. All these concerns are quoted to be vital in the automobile industry. Unfortunately, the state of the art in modeling embedded systems in the context of the automotive engineering does not yet allow the designer to take the best possible advantages

from model-based development. In fact, even if modeling is current practice for today's automotive systems designers, models are still considered as simple description and communication media, although in the context of hard competition that rules the automotive industry, modeling can unacceptably continue to be a task that unnecessarily consumes time instead of being helpful and easy.

Hence, even though models are abstractions of the reality, useful specifications must highlight the system characteristics, motivate the design options and facilitate the design decisions. Therefore, a model should bear all necessary information needed for the subsequent design operations. In the context of embedded systems design, one of the most decisive design operations is the design of the system's architecture. We call this task the partitioning. This paper presents a framework for the evaluation and the classification of the modeling solutions that address the AES domain regarding their ability to support the activities of the implementation phase, in particular the partitioning. Even if a comparison might be expected to be supported by quantitative techniques, this paper limits the scope of the framework on the qualitative analysis of the involved modeling solutions. This is sufficient to enable suggestive evaluations with regard to the AES domain.

2 Problem Definition and Motivation

The overall goal of modeling is to build the system. With a model-based design approach, models are expected to guide the whole design process. That means that all the activities within the life cycle of an AES, from its conception to its destruction, must be supported by models as far as possible. Thus, here, models are the primary artifacts in the system development process. The electronics of AES consist of ECUs, sensors, actuators, gateways and several communication networks. Thanks to the global connectivity enabled by the gateways, these complex, modular and heterogeneous systems can work like a unified system. For example, a power-train member function can communicate with the infotainment system to order the emission of audio signals corresponding to a particular alert. During the design of such systems, decisions must be made about the composition and the topology of the platform on which the system's application will run as well as its implementation. An optimal material usage can considerably reduce the cost and enhance the reliability of AES. As the functionalities of an AES can be implemented on different architectures built each of different hardware components, the choice of the hardware and a goal-oriented partitioning are decisive for both the economy and the performance of the system. Design space exploration allows designers to find optimal implementations of the system by analyzing various alternatives of both the architecture and the topology.

The partitioning of an AES aims at founding the best platform (i.e. hardware components, system's architecture and topology) and distributing the system's working load within the available resources in a manner that the functioning of the system is optimized, by concurrently avoiding resource underutilization. This activity includes three operations: The allocation, i.e. the choice of the

components of the infrastructure platform, the mapping, i.e. the assignment of the elements of the functional specification to the components of the platform and the deployment, i.e. the distribution of the available computing power and the storage capacity of the platform among the elements of the functional model. As shown in figure 1, the mapping is achieved by a clustering that groups the elements of the functional specification of the AES system that should be implemented together in order to profitably share the allocated resources. It results into clusters of functions that represent the logical devices of the system. As these devices communicate through bus networks, the inter-cluster communication can concurrently be assigned to the communication channels of the buses.

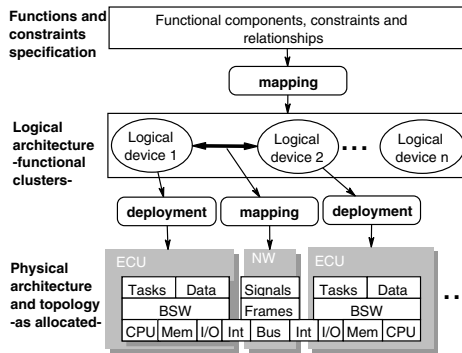


Fig. 1. The partitioning

The goal of the deployment is to assign the computation tasks to the processing units and the logical data to the physical memories in a way that the resource usage is optimized within the required performance and the system constraints (e.g. size, weight, power consumption, safety, speeding up, maintenance, etc.). This operation relies on the scheduling of the tasks on the processing units, the scheduling and the synchronization of the communication within each ECU and the data access procedures. A feasible mapping must allow executable scheduling of the tasks on the containing devices and enable smooth inter-device communications. Thus, in addition to the resource needs and the timing behaviors of the elements of the functional model, the mapping relies on the quality of the information about the inter-components communication and a wide range of relationships between the elements of the functional specification, such as those induced by the strategic concerns of the AES design. AES-desired input specifications must thus enable to clearly identify the boundaries and the interfaces between the components, identify the connection paths, extract the substance and the heaviness of the communications (e.g. throughputs, access rates, data density, timeliness, priorities, security levels, etc.), find out the dependences and causality relations such as sequentiality, concurrency and synchronization, and analyze the internal behaviors of the components (so that their elementary operations and critical paths can be identified) and the relationships resulting from

the strategic concerns of the design. However, the quality of the partitioning depends on the information that is available in the input models. The designer needs powerful and expressive models.

In the current practice, the partitioning is done manually by highly experienced designers, usually called system integrators. When partitioning the system, a system architect must take hundreds of often contradictory, opposite and competitive constraints into account. Keeping this information for a long time in mind is not easy for a human intelligence. A CAD-supported partitioning will be an effective contribution to the dream of model-based system design in the automobile industry. Automated partitioning will be time saving, deterministic and produce well-documented and optimal system architectures. The existing approaches for automated partitioning input very low-level, fine-granular specifications (e.g. logical and arithmetical operations or simple assignments). Unfortunately, because of the complexity of AES, this dimension of granularity is difficult to achieve when following a system-oriented design scheme. As a special domain of interest, important works have addressed the modeling of AES, producing appreciable results. Near general-purpose embedded systems-qualified tools (UML, MatLab, Simulink, SDL,...), more domain-specific modeling solutions have been proposed for the development of AES (e.g. EAST-EEA[1], AADL[2], AUTOSAR[3], etc.). But the most of the known solutions were merely focused on the definition of modeling languages, neglecting the substance of modeling itself and its potential methodological support for the design process.

As each of these solutions pretends to be optimized to support the implementation, it is necessary to investigate the level of support that they provide to the system architects in order to determine how they can be optimally used or how they can be enhanced. We resume this work with the following questions: Which information is needed in a specification to support the partitioning? Which modeling features are needed to provide this information? Do the actual modeling solutions provide these features? How capable are the usual modeling solutions? The rest of the paper is organized as follows: In section 3 we scan the most significant preceding efforts in the evaluation and the classification of embedded systems modeling solutions. In section 4, we define our framework for the classification of AES modeling solutions. Section 5 defines the criteria on which the level of support provided to AES architects will be evaluated. In section 6, we succinctly introduce the most common AES-used modeling solutions, including e.g. UML, SDL, SysML, EAST ADL and AUTOSAR, that are then evaluated and categorized following our framework.

3 Related Work

The aim of the evaluation or the classification of modeling techniques is to measure and compare their potential level of support, their adequacy and their usefulness regarding the requirements of the intended design activity, in our case the partitioning. During the partitioning, the decision-making is based on the

attributes of the model elements like their resource consumptions, their sizes, their need for computation power, their consumption of energy, the magnitude of their collaborations with each other and a lot of other significant interdependencies. To enable the incorporation of the necessary information in the models, a modeling technique must provide a certain level of precision for structuring paradigms, computation paradigms, control paradigms, communication paradigms and for the specification of the constraints and the non-functional requirements.

Several frameworks have been proposed for the evaluation and the classification of embedded systems specification tools. The authors of [4] proposed a classification framework based on five specification styles: State-oriented (using state machines), activity-oriented (using transformations), structure-oriented (concentrating on structural architectures), data-oriented (based on information modeling) and heterogeneous. This classification is mainly based on syntactic criteria. However, it can be used to select a specification style depending on the nature of the behavior that needs to be captured. In contrast, the authors of [5] argue for a classification based on the model of computation (MOC) of embedded systems modeling solutions. Using the Tagged-Signal Model (TSM) [6], a formalism for the description of MOCs aspects, they focus on timing, concurrency and communication aspects to analyze and classify several MOCs. Since a MOC formalizes the execution model of a modeling solution rather than the style in which the specifications are written, this orientation is more objective than the syntax-based classification and is also better adapted to estimate the usefulness of a model. But, generally, as the user is not aware of the MOC of a solution, he also cannot be a priori aware of its quality. A good implementation (i.e. easy and clear syntax, powerful tool support) of a poor MOC is generally far more easily accepted by the user than a poor implementation of a good MOC. MOCs are important characteristics of modeling solutions that cannot be ignored when evaluating them. But, an exclusive orientation on the MOCs is not sufficient for our purpose.

Considering the characteristics of the modeling tools from a very different perspective, Hartenstein [7] used four high-level criteria to classify hardware description languages (HDL): The abstraction level, the application area, the dimension of notation and the source medium of the language. Following this author, the abstraction level characterizes the methodological level for which the language has been designed. The area of application is the type of behavior for which the modeling technique has been defined. The dimension of notation is the general class of information supported, e.g. behavioral, structural or morphological information. The source medium is the presentation medium, e.g. graphic or textual presentation. This framework is right in our target. Its main advantage is its simplicity. But, in order to evaluate AES modeling techniques, we need supplementary dimensions of criteria.

The authors of [8] first identified four main classes of computation models defined on the vectorial cross product of concurrency (control-driven, data-driven) and synchronization (single-thread, distributed). Then they defined three

high-level criteria to compare embedded systems specification languages, i.e. the expressive power, the analytical power and the cost of use. The expressive power determines the level of efforts invested when describing a given behavior. The analytical power measures the level of analysis, transformation and verification facilities offered by the language. The cost of use is composed of aspects like the clarity of the models, the quality of the related existing tools, etc. Even though these criteria are very realistic for the evaluation of embedded system modeling languages, this taxonomy is very abstract and limited regarding the characteristics of AES. Furthermore, although it allows to consider important AES modeling features such as timing and concurrency as first class quality criteria of specification languages, the components-based character of AES is not fungible in this taxonomy. A look into a far different research community lets us discover a framework for the classification and the comparison of architecture description languages (ADL) [9] that can efficiently enhance the taxonomies mentioned in [4,7] and [8] with regard to the AES modeling requirements.

4 The Classification Framework

The modeling solutions that are used in the AES design can be distinguished following their individual originating specialization, i.e. the fields of activity for which the solution has been developed, e.g. general purpose, automotive-specific solution, etc. Independently of its specialization, a modeling solution is conceived with focus on a particular domain of application or to address some problems that are specific to some abstraction/conceptual levels, for example some modeling techniques are optimized for abstract descriptions while others are more effective for more detailed, fine-grained descriptions. Also, a technique may be optimized to specify only the interactions between the system's modules, but not the computation performed in the modules while another one is designed only to specify the causality and constraints of the interactions without detailing the interactions themselves. We retain 5 domains of application to classify AES modeling solutions: The modeling of the requirements, the modeling of the architectures, the modeling of the computations, the modeling of the communications and the modeling of the constraints and the non-functional requirements. The most modeling solutions cover a scope of several domains of application. However, for each domain, the modeling techniques differ in the modeling style, the expressiveness, the granularity and the cost of use.

The modeling style indicates the style of writing the models when using a modeling technique, e.g. architecture-oriented models may use object- or component-based techniques while behavior descriptions may vary between algorithmic descriptions, differential equations, state- or activity-based models, etc. A classification based on the modeling style can be used to localize the most adequate modeling techniques according to the nature of the system under construction.

The expressiveness of a modeling technique determines its appropriateness and its usefulness when capturing the characteristics of a specific system. A modeling technique that is not expressive enough to specify a particular item is

evidently unsuitable. On the other side, a modeling technique in which the item of interest cannot be described succinctly is also problematic. The expressiveness of a modeling technique is evaluated based on the suitability of the concepts it supports regarding the nature of the information that is to be captured. The suitability is determined by the ease to describe the system and the clarity that can be achieved. The components of the expressiveness include for example the ability to model the system structures, the support for the modeling of non-software components, the ability to model the computations and the communications, the handling of time and data, the ability to describe concurrency, synchronization and non-functional requirements, etc.

The granularity determines the dimension of the objects described. In other words, it is the (mean) size of manageable information contained in the elements of the models. The size of the objects it manipulates has great influence on the accuracy that a modeling technique can provide. The granularity is measured on the resolution and the level of precision that are achievable with a modeling technique. Coarse granular solutions are efficient for high-level abstract modeling while fine granular ones are more adequate for detail and low-level modeling.

The AES development is a "team-sport" in which different actors coming from different technical domains act in synergy across different OEMs and suppliers with different points of interest. A modeling technique must be easy to learn and use, intuitive, capable to capture and visualize domain-specific items, but related to standards and at the best leaning onto formal notations. These features determine the cost of use of a modeling technique. The cost of use may include further components like the support of CAD tools, e.g. for edition, syntax check, etc., the executability, the synthesizability, the interoperability with other modeling tools, the affinity with the standards and the visualization medium.

However, even modeling solutions that address the same domain of application and that are deemed adequate for the same conceptual level would differently support the partitioning. The following section presents our framework to capture such differences.

5 Evaluating the Level of Support

The four dimensions of the domains of application mentioned in section 4 might be sufficient to classify the AES candidate modeling solutions, but they are still very abstract to enable an evaluation of the level of support that may be provided. The following taxonomy defines the criteria that indicate the value of a given modeling technique with regard to the partitioning. Depending on the goal of the evaluation, e.g. finding the most adequate, the most useful solution or the one with the best support, a particular combination of these criteria will give the orientation to choose the most appropriate technique.

*Modularity: Independently of the domain of application, the modeling style and the expressiveness, each AES modeling solution should provide some modularization features. The modularity support measures the ability to model the structure and the composition of the system. The modularity is independent

of the granularity. But, it is an important characteristic of the expressiveness and the modeling style of components-based modeling techniques. Concerning the AES design, clear structuring is provided when the system components are clearly identifiable as detachable building blocks with clear boundaries and interfaces. Fuzzy structuring in contrast denotes the difficulty to identify the components and their boundaries. We evaluate the modularity of AES modeling solutions based on the features provided to specify the system's modules and the connections between them. This includes the substance, the encapsulations and the interfaces of the system modules and their connections.

- The substance: A component is normally designed to fulfill a given functionality/service. Both the achievement of a component and its contents must be modeled. The substance of a component defines its role and its composition. A component may be an atomic or a composite structure.

- The interfaces: The interface of a component depends on the way it is encapsulated. Modeling the interface of a component includes the definition of its points of interaction, what it consumes, what it produces, the constraints on these items and the commitments that are necessary to access them, i.e. the type of information that can be consumed and the protocols allowed to be used for the information exchange. Some techniques encapsulate the components using wrappers and virtual interfaces that adapt the communication semantics of the components to the needs of its accessors [10]. Other techniques use special connection components like in [11] where an object-oriented approach is presented with an elegant coordinator concept in which the communication of a composite function is controlled by a coordinator. With this method, the coordinator of a component acts like its communication intelligence. Indeed the coordinator is an intrinsic part of the component. Thus the component's behavior and its communication are always intertwined, making it particularly difficult to separate them and thus to reuse the component since any instantiation of such a component will require to adapt either the accessing components in the destination model or the coordinator, that means the component itself. In the worst case, both must be redesigned. To separate the communication from the behavior, the most methods propose (in- and output) ports. These methods differ in the power they give to ports and the precision of ports descriptions. Some ports are able to transform data, thus holding complex functionalities. Ports can receive directions, types, etc., that simplify the analysis and the synthesis.

*Resolution of the components: The resolution of a component refers to the granularity of the leaves in its hierarchical structure. A leaf component can be as large as the entire system or as small as a logical operation, an arithmetical operation or a simple assignment.

*Computation modeling: A partitioning process will cluster the functions depending on their cost (i.e. computation time, response time), their size, and further attributes like those considering the environment they need to run efficiently (e.g. type of hardware, shareable data, etc.). Therefore, detailed internal behaviors of components are first-class information for the partitioning, that must be precisely specified. The computation description facilities of a modeling

solution are characterized by the type of description used to specify the computations and the provided level of detail. This encompasses the modeling style, the granularity and the expressiveness of these models.

*Communication and data modeling: The attributes of the information exchanged and the protocol governing the communication strongly constrain the partitioning. AES communication may be synchronous or asynchronous, realized by direct information passing or shared memory, in P2P or multi-cast schemes. At different levels of abstraction, the substance of a communication may be specified in terms of services or operations invocations, messages or data block passing, signals or bits flows, etc., and the communication primitives may vary between call/request, send/receive, read/write, set/reset, load/save, etc. The evaluation of the capability of a modeling technique to model the communication is based on the types of communication supported (cf. expressiveness and cost of use), the tools used to capture the communication (cf. modeling style and cost of use) and the resolution (cf. granularity) of the information exchanged.

*Time modeling: Timing information modeling is crucial for embedded systems. The ability of a modeling technique to model time is evaluated through its conceptualization of the notion of time and the resolution of time expression. Time can be expressed through ordering of the activities in the processing (i.e. the order in which things happen induces a notion of time), or as absolute values measured by a clock, this at different resolutions. A modeling technique that can achieve high resolution in modeling timing behaviors is suitable for the partitioning.

*Concurrency and synchronization: Embedded systems behave inherently concurrently. Concurrency has two forms: parallelism and interleaving. Parallel processes run at the same time. They may need to communicate and synchronize, for example to publish their beginnings and ends. Interleaving processes must compete for resources. In order to coordinate the interaction of concurrent processes, some intelligent synchronization mechanisms such as schedulers, message queues (buffers), rendez-vous (for message passing), semaphores or read/write blocking in the case of shared memory are needed. The evaluation of the ability of a modeling solution to model concurrency and synchronization is based on the number of concurrency schemes and synchronization mechanisms that are supported and the quality of the concepts that are proposed to capture them.

*Relation to standards: The distance between a given modeling solution and the nearest standards is an important factor for its acceptance. The relation to standards determines the intuitiveness of a solution, the facility to learn and to communicate it and the possibility to integrate it with other solutions.

*Executability and synthesizability: The executability of a modeling solution refers to the existence of a tool that can be used to simulate the behavior of a system described with this solution. Synthesizable means that there exists a tool that can translate a specified behavior into a machine code or a netlist level model from which properties like memory consumption, hardware size, execution time, etc. can be directly measured. Low-level modeling techniques generally have efficient compilers or synthesis tools that allow rapid

prototyping. Some sophisticated high-level models may be executable, particularly when based on formal definitions. Executable and synthesizable modeling solutions have advantageous cost of use.

*Abstraction levels: Measures the ability to support different AES domain-established methodological and conceptual abstraction levels.

*Support for variance handling: Depends on the quality of the features provided to support the design of product lines. This includes the modeling of varying elements and of the configuration information.

6 Evaluation and Classification of AES Modeling Languages

Besides the modeling techniques, modeling languages are needed to express the contents of the models. AES modeling solutions generally incorporate each a language that in the reality becomes such a prominence that the whole modeling solution is generally called modeling language. The spectrum of AES-usable modeling languages is very wide, going from general-purpose programming languages and hardware description languages (HDL) to architecture description languages (ADL) and other more promoted languages such as UML, SDL, SysML, EAST ADL, AUTOSAR. General-purpose programming languages, e.g. *C*, *Assembler*, *C++*, *Pascal*, *Fortran*, *Java*, etc. are also widely used to specify embedded systems. Similar to HDL (most known in the area of HW/SW co-design, e.g. *VHDL*, *Verilog*, *System Verilog*, *System C* and *Esterel*), they are optimized for fine-granular design. In contrast to ADLs, both programming languages and HDLs provide executable models and possess proved stable compilers, but they are too close to the implementation and they provide poor abstraction capabilities. SDL, usually used in combination with MSC, ASN.1 and TTCN (ITU standards Z.105, Z.107), provides good message communication and time modeling features as well as an appreciable support of synchronization and good abstraction possibilities. But, since it is OO-based, SDL offers very poor modularization of the system under design.

Since the OMG adopted real-time and embedded systems optimized concepts, e.g. components, events, actions, resources, schedules and timing to enable the high-level design of embedded systems, the UML is becoming popular in the field of the embedded systems software design. However, although UML may provide a modeling power that is suitable to capture the behavior of AES, it does provide neither synthesizable models nor meaningful support for model analysis. Furthermore, UML does not support the AES domain-specific concepts such as the specification and the management of the requirements, the product lines, the configurations, the transitions and the hardware resources. Inspired from UML, SysML adds a requirements diagram to the structure, allocation and behavior diagrams existing in UML. Parametric diagrams are used in SysML to specify the performance, reliability, safety, cost properties of the system under construction, etc. that can support the engineering and trade-offs analysis, thus the partitioning. In addition to these features, EAST ADL defines several conceptual levels

while AUTOSAR promotes the standardization of AES' software components and their interfaces. But, although these languages (i.e. based on UML) provide strong modeling power that can be sufficient to describe the most artifacts of the AES at the high-level, they may not always match the AES architects' ideas as faithfully as desired.

High resolution, clear encapsulation, execution and synthesis tools are needed in both the high- and the low-level design while clear modularity is essential in the higher levels. When the design follows a top-down strategy, none of the above languages can be expressive enough to be used efficiently for all purposes along the design process, since each of them offers in reality only a limited set of features. Otherwise, we are not aware of the existence of such an all-rounder general-purpose modeling language. However, the partitioning of AES needs clearly-framed functional components with their resource consumption properties, their communication paths, their timing behaviors as well as those of the communication between them. Following these requirements for the partitioning, we can classify the studied languages into two groups: Those that are more adequate for the high-level modeling and those that are more adequate for the low-level modeling. The first group contains UML, SysML, EAST ADL, AUTOSAR and the other ADLs, well-suited for the needs of the high-level design. These languages provide powerful architectural modeling features enabling components detachability, but they lack synthesizability. The second group is populated with the programming languages, the HDLs and all kinds of languages that are similar to those used in Matlab, Simulink, Statemate, ASCET-MD, etc. These languages with high resolution, execution and synthesis tools easily fulfill the requirements related with the executability and the synthesizability required for partitioning-compliant languages, but they are unfortunately too fine-grained and only provide fuzzy structuring capabilities, thus being less efficient in the high-level design. Consequently, at each step of the development process, the most adequate language must actually be selected depending on the current conceptual layer, the level of abstraction and the intended use of the model.

However, in addition to the concepts related with the components orientation, the behavior and the interaction description tools borrowed from the UML, the AES domain-specific languages (e.g. EAST ADL and AUTOSAR) and SysML commonly address the domain issues like variants handling, configurations management, hardware platforms modeling, support for non-software components and definition of methodological abstraction levels. This allows them to perform better than the general-purpose ADLs in modeling AES at the high level. They therefore provide a good basis for an efficient AES modeling solution, even if the semantics provided for specifying the ports and the interfaces are not precise enough to support a CAD-supported partitioning. Particularly, the standardization of AUTOSAR interfaces will allow the designer to shift a function from a device to another one, enabling high-level mapping, i.e. partitioning. However, if enhanced with some features allowing for example clear tracing of the inter-components communication paths and the data flow screening, these high-level languages can be very useful for the design of CAD-supported mapping tools.

7 Conclusion

The design of AES begins with high levels of abstraction for which the modeling languages like UML, SDL, SysML, EAST ADL or AUTOSAR are adequate. Even if the syntax is different from one language to another one, most of these languages are based on the idea of components-based systems, i.e. they conceive a system as a set of components communicating through interfaces and ports. All these languages claim sufficient orientation to the implementation, but they still remain very abstract and lack synthesis and execution tools. As domain-dedicated languages, EAST ADL and AUTOSAR provide the most convenient features and the best precision needed to model AES, but they remain very insufficient to support the partitioning of the system. Firstly, because they are not synthesizable. Secondly, the semantics of ports, interfaces and connectors are fuzzy. A promising solution to the first drawback is to combine these languages with low-resolution languages such as programming languages, HDLs, etc. But this will not be the ultimate solution for supporting the partitioning of system specifications at high level. However, if these languages are enhanced with precise computations and communication modeling tools, accurate time and data handling, etc. so that the QoS of the model elements can be extracted and analyzed, then they will represent appreciable solutions to build partitioning-compliant models of AES.

References

- [1] EAST-EEA: Embedded Electronic Architecture. Definition of Language for Automotive Embedded Electronic Architecture v. 1.02, ITEA, Tech. Rep. (30.06.2006)
- [2] AADL, <http://www.aadl.info/>
- [3] AUTOSAR, <http://www.autosar.org>
- [4] Gajski, D., Vahid, F., Narayan, S., Gong, J.: Specification and Design of Embedded Systems. Prentice-Hall, Englewood Cliffs (1994)
- [5] Lavagno, L., Sangiovanni-Vincentelli, A., Sentovitch, E.: Models of Computation for Embedded Systems Design. In: System-Level Synthesis Ch. 2, pp. 45–102. Kluwer Academic Publishers, Dordrecht (1999)
- [6] Lee, E.A., Sangiovanni-Vincentelli, A.: Comparing Models of Computation. In: International Conference on Computer-Aided Design, pp. 234–241 (1996)
- [7] Hartenstein, R.W.: A Comparison of Hardware Description Languages. In: Advances in CAD for VLSI Ch. 2, vol. 7, Elsevier Science Publishers B.V, Amsterdam (1987)
- [8] Jerraya, A.A., et al.: Multilanguage Specification for System Design. In: System-Level Synthesis Ch. 3, pp. 103–135. Kluwer Academic Publishers, Dordrecht (1999)
- [9] Medvidovic, N., Taylor, R.N.: A Classification and Comparison Framework for Software Architecture Description Languages. UCI and USC, Tech. Rep.
- [10] Nicolescu, G., Yoo, S., Bouchhima, A., J.A.A.: Validation in a Component-Based Design Flow for Multicore SoCs. In: Okada, M., Pierce, B.C., Scedrov, A., Tokuda, H., Yonezawa, A. (eds.) ISSS 2002. LNCS, vol. 2609, Springer, Heidelberg (2003)
- [11] Mutz, M., Huhn, M., Goltz, U., Kroemke, C.: Model Based System Development in Automotive. In: SAE (2002)

Security Analysis of the Certificateless Signature Scheme Proposed at SecUbiq 2006

Je Hong Park¹ and Bo Gyeong Kang²

¹ ETRI Network & Communication Security Division
jhpark@ensec.re.kr

² Samsung Electronics Co., LTD
bogyeong.kang@samsung.com

Abstract. In this paper, we show that the certificateless signature scheme proposed by Yap, Heng and Goi at SecUbiq 2006 is insecure against a key replacement attack and a malicious-but-passive KGC attack, respectively. The former implies that anyone who replaces a signer's public key can forge valid signatures for that signer without knowledge of the signer's private key. The latter supposes the malicious-but-passive KGC, which generates system parameters based on the information of the target user to impersonate. Our results are based on the fact that the private key of the YHG scheme has the form of a BLS multisignature generated by the KGC and the user. Finally, we review the vulnerability of several certificateless signature schemes under these attacks.

1 Introduction

The certificateless cryptosystem introduced by Al-Riyami and Paterson [1] is designed to overcome the key escrow limitation which is inherent in identity-based cryptosystems. Each user has a unique identifier, and a semi-trusted third party called the Key Generation Center(KGC) generates the partial private key associated with that identifier using its own master secret key and sends it to the user with that identifier. But the user also holds a secret value which is chosen by him/herself, and the user combines the partial private key with the secret value to generate his/her actual private key. That is, the user's private key is not generated by the KGC alone and so the KGC does not know the user's private key that implies the escrow freeness. Independent to the identifier, the user also publishes the public key, based on the secret value and system parameters. Note that the user's public key does not need to be certified by any trusted authority as in conventional PKIs. The structure of the certificateless scheme ensures that the key can be verified without a certificate. So its security model supposes the adversary who may attempt to replace a user's public key with a value of its own choice. This is called in general a *key replacement attack* [9,418,67] and, successfully applied to some certificateless signature schemes such as [15].

In the original security model for certificateless cryptosystems [1], the KGC generates its master public/private key pair honestly, according to the scheme specification. However, the modified security model proposed by Au et al. [2]

removes this assumption. So the user’s trust on the KGC is further relaxed. In detail, the KGC may not follow the scheme specification for generating system parameters and master key, while it does not actively replace a user’s public key or corrupt the user’s private key. The purpose of such a KGC is to compromise the target user’s private key without being detected. Note that the *malicious* KGC is still *passive*, in the sense that the KGC would not actively replace the user public key or corrupt the user private key. It was shown in [2] that Al-Riyami-Paterson scheme [1] and Huang-Susilo-Mu-Zhang scheme [9] are vulnerable in this security model.

In SecUbiq 2006, Yap, Heng and Goi proposed a certificateless signature scheme (called the YHG scheme here) and claimed that their scheme is efficient, comparison to previous schemes [15]. Their improvement is supported by the lack of public key validation which requires pairing computations in the signature verification phase. We, however, show that the YHG scheme is insecure against a key replacement attack and a malicious-but-passive KGC attack, respectively. The former attack is based on the fact that the user private key of the YHG scheme has the form of a BLS multisignature [3] generated by the KGC and the user. We will apply a rogue attack for BLS multisignatures to the YHG scheme: Due to the lack of public key validation in the signature verification phase, a verifier cannot ensure that the signer knows the secret value. It implies that an adversary who replaces a signer’s public key can forge signatures of that signer, without knowledge of the signer’s private key. Additionally, we show that the malicious KGC can generate master public key using the target user’s identifier and so it may impersonate that user easily, as described in [2]. Note that the Gorantla-Saxena scheme [5] and its improved scheme [17] are also vulnerable to this attack, due to structural similarity.

This paper is organized as the follows. We briefly review the YHG scheme in Section 2, and then analyze its security against two types of attacks in Section 3. We conclude in Section 4.

2 Review of YHG Certificateless Signature Scheme

Throughout this paper, $(\mathbb{G}_1, +)$ and (\mathbb{G}_2, \cdot) denote two cyclic groups of prime order q . A *pairing* is an efficiently computable, non-degenerate function $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the bilinearity property that $e(P + Q, R) = e(P, R) \cdot e(Q, R)$ and $e(P, Q + R) = e(P, Q) \cdot e(P, R)$ for $P, Q, R \in \mathbb{G}_1$. Let $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$ and $H_2 : \{0, 1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$ be hash functions. These are used as a part of the system parameters generated by the KGC. The YHG certificateless signature scheme can be described as follows:

- Setup: Given a security parameter k , the KGC chooses an arbitrary generator $P \in \mathbb{G}_1$, selects a random $s \in \mathbb{Z}_q^*$ and sets $P_0 = sP$. Then the system parameters are $\text{params} = \langle \mathbb{G}_1, \mathbb{G}_2, e, q, P, P_0, H_1, H_2 \rangle$. The message space is $\mathcal{M} = \{0, 1\}^*$. The master secret key is $\text{mk} = s$.

- Set Partial Private Key: Given the system parameters params , the master secret key mk and a user A 's identifier ID_A , the KGC computes $Q_A = H_1(\text{ID}_A) \in \mathbb{G}_1$ and outputs the partial private key $D_A = sQ_A$.
- Set Secret Value: Given the system parameters params , the user A selects a random value $x_A \in \mathbb{Z}_q^*$ as the user secret value.
- Set Private Key: Given the system parameters params and the partial private key D_A , the user A computes the user private key $S_A = x_A Q_A + D_A$.
- Set Public Key: Given the system parameters params and the secret value x_A , the user A computes the user public key $P_A = x_A P \in \mathbb{G}_1$.
- Signature Generation: Given the system parameters params , the identifier ID_A , a message $m \in \mathcal{M}$ and the private key S_A , the user A randomly chooses $r \in \mathbb{Z}_q^*$ and sets $U = rQ_A \in \mathbb{G}_1$. Then computes a signature $\sigma = (U, V)$ for the message m where $V = (r + h)S_A$ and $h = H_2(m, U)$.
- Signature Verification: Given a signature/message pair (σ, m) , the signer's identifier ID_A and the signer's public key P_A , the verifier computes $h = H_2(m, U)$ and checks whether $e(P, V) = e(P_0 + P_A, U + hQ_A)$. If not, then rejects the signature else accepts it as valid.

The authors claim that this scheme is provably secure and more efficient than previously proposed schemes because fewer bilinear pairing computations are required [15]. As described above, this scheme requires only two pairing computations in the signature verification phase. This efficiency is induced from the lack of public key validation. We will show that this fact makes the YHG scheme vulnerable to the key replacement attack.

3 Security Analysis

3.1 Key Replacement Attack

Without loss of generality, the signer forwards his/her public key to the intended verifier(s) and announces his/her identifier. So an adversary who wants to forge a signature of a user A with the identifier ID_A runs as follows:

1. Randomly chooses $x \in \mathbb{Z}_q^*$ and computes a signature $\sigma = (U, V)$ for a message $m \in \mathcal{M}$ as follows:

$$U = rQ_A, h = H_2(m, U) \text{ and } V = (r + h)xQ_A,$$

where $Q_A = H_1(\text{ID}_A)$ and $r \in \mathbb{Z}_q^*$.

2. Sets $P'_A = xP - P_0$ as a public key of the user A .
3. Then sends the signature σ , the message m , the identifier ID_A and the public key P'_A to the verifier(s).

Then the verifier computes $h = H_2(m, U)$ and checks whether $\langle P, P_0 + P'_A, U + hQ_A, V \rangle$ is a valid Diffie-Hellman tuple. Since $e(P, V) = e(P, (r + h)xQ_A)$ and $e(P_0 + P'_A, U + hQ_A) = e(xP, (r + h)Q_A)$, $e(P, V) = e(P_0 + P'_A, U + hQ_A)$ and so $\langle P, P_0 + P'_A, U + hQ_A, V \rangle$ is valid. Hence σ is verified as a valid signature for the message m generated by the user A .

This attack is based on the algebraic structure of a user’s private key in the YHG scheme. Since the signer A ’s private key S_A has the form of a BLS multisignature [3] generated by the KGC and the signer A , we can apply a rogue attack using the key substitution trick. In general, a rogue attack for BLS multisignatures can be described as follows: Let $pk_A = x_A P$ and $pk_B = x_B P$ be two public keys of the user Alice and Bob, respectively. But Bob replaces pk_B by $pk_B - pk_A$. Then for a message m , $x_B H_1(m) = x_A H_1(m) + (x_B - x_A) H_1(m)$ can be regarded as a valid multisignature on m by both Alice and Bob. In the YHG scheme, the KGC plays the role of a honest user to generate a multisignature for the identifier ID_A of a user A and is prohibited to replace the user A ’s public key. But a third party can use this key substitution trick for BLS multisignatures to forge a YHG signature of the user A , based on two facts that the user A ’s public key is not certified and knowledge of the secret value corresponding to the signer’s public key is not, even implicitly, checked in the signature verification phase.

To prevent this attack, therefore, the signature verification phase is required to demonstrate that the signer has knowledge of the secret value corresponding to the public key [4]. One instance to provide it is to modify the public key of a user A to include an additional value $x_A P_0$, where x_A is the secret value of the user A and then to add the public key validity check equation

$$e(P_0, P_A) = e(P, x_A P_0) \tag{1}$$

to the signature verification phase [4]. This equation basically ensures that the signer A ’s public key $\langle X, Y \rangle$ holds the relation $Y = sX$ where $Y = x_A P_0$ and $X = P_A$. Furthermore, it makes sure that the secret value x_A , chosen by the signer A , has been used correctly to obtain $S_A = x_A Q_A + D_A$ [6][7]. Though an adversary is able to replace the public key P_A by P'_A , it is impossible to pass the equation (1) without knowledge of the discrete logarithm of P'_A . Unfortunately, this modification requires four pairing computations though only two are needed per signature if multiple signatures by the same signer are to be verified. Note that this modification only provides a way to defend our attack, and so does not guarantee the security against other attacks [8]. We provide such an example in the following subsection.

Remark 1. Independently, the same attack for the YHG scheme was proposed by Zhang and Feng [16], after we published a preliminary version of this paper [14]. While our attack chooses a random exponent $r \in \mathbb{Z}_q^*$ to construct U , they choose $U \in \mathbb{G}_1$ itself as a random factor of a forged signature $\sigma = (U, V)$. Since $V = (r + h)xQ_A = x(U + hQ_A)$, there is nothing to differentiate between two attacks.

3.2 Malicious-but-Passive KGC Attack

Although the above key replacement attack can be prevented by additional checking process, the following malicious-but-passive KGC attack is still applied to the (modified) YHG scheme. Note that this attack is not captured in [15]

because the security of the YHG scheme is only considered in the original security model of [1], but not of [2].

At first, fix a target user A with the identity ID_A . Then the malicious KGC randomly chooses $\alpha \in \mathbb{Z}_q^*$ and computes $P = \alpha H(ID_A)$. Then the user A computes his/her public key and private key pair as follows:

$$\begin{aligned} P_A &= x_A P = x_A \alpha H(ID_A) \\ S_A &= x_A Q_A + D_A = x_A (1/\alpha) P + D_A = (1/\alpha) P_A + D_A. \end{aligned}$$

Since the KGC knows α , P_A and D_A , the private key S_A of the user A can be easily computed by the malicious KGC. As a result, we show that the (modified) YHG scheme is weak against the malicious-but-passive KGC attack though the scheme does not have the same key generation procedure as that of [1].

Remark 2. The Gorantla-Saxena scheme [5] and its improved scheme [17] have a similar structure with the YHG scheme. So, it is very easy to check that both schemes are also vulnerable to a malicious-but-passive KGC attack.

Besides [11,9], it was shown that certificateless signature schemes in [12] and [13] are insecure against the malicious-but-passive KGC attack [8]. Additionally, the certificateless designated verifier signature scheme proposed by Huang et al. is vulnerable to the malicious-but-passive KGC attack as they follow the same system parameters and user key generation procedure as that of [1].

It can be easily checked that the mediated certificateless signature scheme proposed by Ju et al. [11] is vulnerable to key replacement and malicious-but-passive attacks. A mediated certificateless signature scheme uses an online semi-trusted entity called the Security Mediator(SEM) for easy revocation of the user signing key. Since a key replacement attack is not related to the partial private key generated by the KGC (and shared by the user and the SEM), the attack in [9] is applied to the Ju et al.'s scheme directly. Similarly, a malicious-but-passive KGC attack in [2] also works because the SEM does not participate in the system parameters generation phase.

4 Conclusion

We showed that the YHG certificateless signature scheme is vulnerable to a key replacement attack and a malicious-but-passive attack, respectively. In addition, we pointed out the same weakness of several certificateless signature schemes under these attacks.

References

1. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003)
2. Au, M.H., Chen, J., Liu, J.K., Mu, Y., Wong, D.S., Yang, G.: Malicious KGC attacks in certificateless cryptography. In: Proc. of ASIACCS 2007, pp. 302–311 (2007)

3. Boldyreva, A.: Efficient threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellman-group signature scheme. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 31–46. Springer, Heidelberg (2002)
4. Cao, X., Paterson, K.G., Kou, W.: An attack on a certificateless signature scheme. Cryptology ePrint Archive, Report 2006/367
5. Gorantla, M.C., Saxena, A.: An efficient certificateless signature scheme. In: Hao, Y., Liu, J., Wang, Y.-P., Cheung, Y.-m., Yin, H., Jiao, L., Ma, J., Jiao, Y.-C. (eds.) CIS 2005. LNCS (LNAI), vol. 3802, pp. 110–116. Springer, Heidelberg (2005)
6. Hu, B.C., Wong, D.S., Zhang, Z., Deng, X.: Key replacement attack against a generic construction of certificateless signature. In: Batten, L.M., Safavi-Naini, R. (eds.) ACISP 2006. LNCS, vol. 4058, pp. 235–246. Springer, Heidelberg (2006)
7. Hu, B.C., Wong, D.S., Zhang, Z., Deng, X.: Certificateless signature: A new security model and an improved generic construction. Des. Codes. Crypt. 42, 109–126 (2007)
8. Huang, X., Mu, Y., Susilo, W., Wong, D.S., Wu, W.: Certificateless signature revisited. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, Springer, Heidelberg (2007)
9. Huang, X., Susilo, W., Mu, Y., Zhang, F.: On the security of certificateless signature schemes from Asiacrypt 2003. In: Desmedt, Y.G., Wang, H., Mu, Y., Li, Y. (eds.) CANS 2005. LNCS, vol. 3810, pp. 13–25. Springer, Heidelberg (2005)
10. Huang, X., Susilo, W., Mu, Y., Zhang, F.: Certificateless designated verifier signature schemes. In: Proc. of AINA 2006, pp. 15–19 (2006)
11. Ju, H.S., Kim, D.Y., Lee, D.H., Lim, J., Chun, K.: Efficient revocation of security capability in certificateless public key cryptography. In: Khosla, R., Howlett, R.J., Jain, L.C. (eds.) KES 2005. LNCS (LNAI), vol. 3681, pp. 453–459. Springer, Heidelberg (2005)
12. Li, X., Chen, K., Sun, L.: Certificateless signature and proxy signature schemes from bilinear pairings. Lithuanian Mathematical Journal 45, 76–83 (2005)
13. Liu, J.K., Au, M.H., Susilo, W.: Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model. In: Proc. of ASIACCS 2007, pp. 273–283 (2007)
14. Park, J.H.: An attack on the certificateless signature scheme from EUC Workshops 2006. Cryptology ePrint Archive, Report 2006/442
15. Yap, W.-S., Heng, S.-H., Goi, B.-M.: An efficient certificateless signature scheme. In: Zhou, X., Sokolsky, O., Yan, L., Jung, E.-S., Shao, Z., Mu, Y., Lee, D.C., Kim, D., Jeong, Y.-S., Xu, C.-Z. (eds.) EUC 2006. LNCS, vol. 4097, pp. 322–331. Springer, Heidelberg (2006)
16. Zhang, Z., Feng, D.: Key replacement attack on a certificateless signature scheme. Cryptology ePrint Archive, Report 2006/453
17. Zhang, J., Mao, J.: Security analysis of two signature schemes and their improved schemes. In: Gervasi, O., Gavrilova, O. (eds.) ICCSA 2007. Part I. LNCS, vol. 4705, pp. 589–602. Springer, Heidelberg (2007)
18. Zhang, Z., Wong, D.S., Xu, J., Feng, D.: Certificateless public-key signature: Security model and efficient construction. In: Zhou, J., Yung, M., Bao, F. (eds.) ACNS 2006. LNCS, vol. 3989, pp. 293–308. Springer, Heidelberg (2006)

New Efficient Certificateless Signature Scheme*

Lei Zhang¹, Futai Zhang¹, and Fangguo Zhang²

¹ College of Mathematics and Computer Science,
Nanjing Normal University, P.R. China

² Department of Electronics and Communication Engineering,
Sun Yat-Sen University, Guangzhou 510275, P.R. China
lei_zhangzl@126.com, zhangfutai@njnu.edu.cn,
isszhfg@mail.sysu.edu.cn

Abstract. In ubiquitous computing environment, how to implement security and trust among the users that connected to a network is a big problem. Digital signature provides authenticity, integrity and non-repudiation to many kinds of applications in ubiquitous computing environment. In this paper, we present a very efficient certificateless signature scheme from bilinear maps. In our scheme, only one paring operation is needed in the signing and verification processes. The security of the new scheme is based on the intractability of the q -Strong Diffie-Hellman (q -SDH) Problem and the Discrete Logarithm Problem. We prove the existential unforgeability of our scheme under adaptively chosen message attack against both types of adversaries in the random oracle model [3].

Keywords: cryptography, certificateless signature scheme, bilinear map, random oracle model.

1 Introduction

To provide the binding between a singer and his public key, the traditional public key signature uses a certificate that is a digitally signed statement issued by the CA. Such certificate can be verified by anyone and guarantees the authenticity of a user's public key. In implementation, the management of public key certificates requires a large amount of computation, storage, and communication cost.

To lower such cost for public key certificate, Shamir [15] proposed another approach named "Identity Based Public Key Cryptography (ID-PKC)" in 1984. In this new approach, a user's public key can be an arbitrary bit string which can represent the user's identity, such as his telephone number or his email address, etc. And the user's corresponding private key is computed by a trusted authority who is referred to as the "Private Key Generator (PKG)" [2,5,12,16]. On input a user's identity and the secret master key owned by PKG, the PKG

* Project supported by the nature science foundation of China (No. 60673070), the nature science foundation of Jiangsu province (No. BK2006217), and the open project of the key Lab. on computer networks and information security (Xidian University) of ministry of education of China (No. 20040105).

outputs the user's private key. In this setting, the public key of a user is just his identity, and no public key certificate is needed. It provides implicit certification of a user's public key based on the fact that only when the user gets a correct private key corresponding to his published identity can he perform some cryptographic operations using his private key. However, there is a basic assumption in identity based cryptosystem, that is the PKG is unconditionally trustable. This is because the PKG knows the private key of every user in the system. So ID-PKC is suffering from the key escrow problem.

To overcome the drawback of key escrow in ID-PKC, Al-Riyami and Paterson [1] proposed a new paradigm called certificateless public key cryptography in 2003. Like ID-PKC, certificateless cryptography does not use public key certificate [1][11][18], it also needs a third party called Key Generation Center (KGC) to help a user to generate his private key. However, the KGC does not have access to a user's full private key. It just generates a user's partial private key from the user's identity as the PKG in ID-PKC does. A user computes his full private key by combining his partial private key and a secret value chosen by himself. The public key of a user is computed from the KGC's public parameters and the secret value of the user, and it is published by the user himself.

Recently, many researchers have been investigating secure and efficient certificateless signature schemes. In their original paper [1], Al-Riyami and Paterson presented a certificateless signature scheme. Huang et al. [9] pointed out a security drawback of the original scheme and proposed a secure one. They also defined the security model of certificateless signature schemes in the same paper. Zhang et al. [21] improved the security model of certificateless signature schemes, and presented a secure certificateless signature scheme. In [18], Yum and Lee presented a generic way to construct certificateless signature schemes, however, Hu et al. [8] pointed out that this construction is insecure and presented a new one. Gorantla and Saxena [7], Yap, Heng, and Goi [17] also presented some efficient certificateless signature schemes. Unfortunately, their schemes [7][17] are subject to universal forgery, a type I adversary can forge signatures on any message [6][13][19]. With respect to the efficiency, the previous certificateless signature schemes all involve a relatively large amount of pairing computation in the process of verification.

Our contribution. In this paper, we present a new efficient certificateless pairing-based signature scheme, yielding some advantages over previous constructions [7][9][10][17][21] in computational cost. Our signature scheme requires only one pairing operation in the signing and verification phases, so it is much more efficient than the schemes in [7][9][10][17][21]. The security of our scheme is based on the hardness of q -Strong Diffie-Hellman (q -SDH) Problem and the Discrete Logarithm (DL) Problem.

Paper organization. The rest of the paper is organized as follows. Section 2 gives some preliminaries, including bilinear maps, our complexity assumptions, the notions of certificateless signature schemes and their security models. Our new efficient certificateless signature scheme comes in Section 3. In Section 4, we prove the security of our new scheme. The efficiency of our new scheme

is compared with some existing certificateless signature schemes in Section 5. Finally, Section 6 comes our conclusion.

2 Preliminaries

2.1 Bilinear Maps and Related Complexity Assumptions

Let G_1 be an additive group of prime order p and G_2 be a multiplicative group of the same order. Let P denote a generator of G_1 . A mapping $e : G_1 \times G_1 \rightarrow G_2$ is called a bilinear mapping if it satisfies the following properties:

1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for $P, Q \in G_1, a, b \in Z_p^*$.
2. Non-degeneracy: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3. Computable: There exists an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$.

A bilinear pairing instance generator is defined as a probabilistic polynomial time algorithm \mathcal{IG} that takes as input a security parameter l and returns a uniformly random tuple (p, G_1, G_2, e, P) of bilinear parameters, where p is a prime number of size (bit-length) l , G_1 and G_2 are cyclic additive and multiplicative groups of order p respectively, $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map, and P is a generator of G_1 . For a group G of prime order, we denote the set $G^* = G \setminus \{\mathcal{O}\}$, where \mathcal{O} is the identity element of the group.

Definition 1. Discrete Logarithm (DL) Problem in G_2 . Given a generator g of G_2 , and $y \in G_2^*$ to find an integer $a \in Z_p^*$ such that $y = g^a$.

The DL problem in G_1 can be defined in a similar way.

Definition 2. The q -Strong Diffie-Hellman (q -SDH) problem in the group G_1 is, given a $(q + 1)$ -tuple $(P, \alpha P, \alpha^2 P, \dots, \alpha^q P)$ as input, finding a pair $(c, \frac{1}{\alpha+c} P)$ with $c \in Z_p^*$.

Assumption 1. The Discrete Logarithm (DL) Problems in both G_1 and G_2 are intractable.

Assumption 2. The q -SDH Problem in G_1 is intractable.

2.2 Certificateless Signature Schemes

A certificateless signature scheme is defined by seven algorithms: Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Sign and Verify. The description of each algorithm is as follows.

- **Setup:** This algorithm accepts as input a security parameter l and returns a master-key and a list of system parameters params . It also defines the message space \mathcal{M} .

- **Partial-Private-Key-Extract:** This algorithm accepts as input a user’s identity ID_i , a parameter list params and a master-key to produce the user’s partial private key D_i .
- **Set-Secret-Value:** This algorithm accepts as input a parameter list params and a user’s identity ID_i to produce the secret value x_i for this user.
- **Set-Private-Key:** This algorithm accepts as input a parameter list params , a user’s identity ID_i , his partial private key D_i and secret value x_i to produce a private signing key S_i for this user.
- **Set-Public-Key:** This algorithm takes as input a parameter list params , a user’s identity ID_i and the secret value x_i to produce a public key P_i for this user.
- **Sign:** This algorithm accepts a message $M \in \mathcal{M}$, \mathcal{M} is the message space, the signer’s identity ID_i and the corresponding public key P_i , a parameter list params and the signing key S_i to generate a signature σ on message M .
- **Verify:** This algorithm accepts a message M , a signature σ , a parameter list params , the signer’s identity ID_i and the corresponding public key P_i to output true if the signature is valid, or \perp otherwise.

2.3 Adversarial Model of Certificateless Signature Schemes

As defined in [1], there are two types of adversary with different capabilities in certificateless signature schemes.

Type I Adversary: This type of adversary \mathcal{A}_I does not have access to the master-key, but \mathcal{A}_I has the ability to replace the public key of any entity with a value of his choice. This is because there is no certificate involved in certificateless signature schemes.

Type II Adversary: This type of adversary \mathcal{A}_{II} has access to the master-key but cannot perform public key replacement.

In this section, firstly we provide a formal definition of existential unforgeability of a certificateless signature scheme against both types of adversaries under chosen message attack. They are defined using the following games between a challenger \mathcal{C} and an adversary \mathcal{A}_I or \mathcal{A}_{II} .

Game 1 (for *Type I Adversary*)

- **Setup:** \mathcal{C} runs the Setup algorithm, takes as input a security parameter l to obtain the master-key and the system parameter list params . \mathcal{C} then sends params to the adversary \mathcal{A}_I .
- **Partial-Private-Key Queries PPK(ID_i):** \mathcal{A}_I can request the partial private key of any user with identity ID_i . In respond, \mathcal{C} replies the partial private key D_i of the user.
- **Public-Key Queries PK(ID_i):** \mathcal{A}_I can request the public key of a user with identity ID_i . In respond, \mathcal{C} outputs the public key P_i .
- **Private-Key Queries Pr(ID_i):** \mathcal{A}_I can request the private key of a user with identity ID_i . In respond, \mathcal{C} outputs the private key S_i .

- Public-Key-Replacement Queries $\text{PKR}(ID_i, P'_i)$: This query is to replace the public key P_i for an identity ID_i with a new value P'_i . On receiving such a query, \mathcal{C} updates the public key to the new value P'_i .
- Sign Queries $\text{S}(M, ID_i, P_i)$: \mathcal{A}_I can request a user's (whose identity is ID_i) signature on a message M . On receiving a query $\text{S}(M, ID_i, P_i)$, \mathcal{C} generates a signature σ on message M and replies with (M, σ, ID_i, P_i) .
- Output: This procedure contains three steps.

Step 1: Select target identity: \mathcal{A}_I selects a target identity ID^* , chooses a new public key P_{ID^*} for this identity. He Submits (ID^*, P_{ID^*}) to \mathcal{C} .

Step 2: Further queries: \mathcal{A}_I can make more Partial-Private-Key, Public-Key, Private-Key, Public-Key-Replacement and Sign Queries.

Step 3: Forge: \mathcal{A}_I outputs a tuple $(M^*, \sigma^*, ID^*, P_{ID^*})$. This tuple must satisfy the following requirements:

 1. σ^* is a valid signature on message M^* for user ID^* under public key P_{ID^*} chosen by \mathcal{A}_I .
 2. \mathcal{A}_I has never asked the partial private key or private key of the user whose identity is ID^* .
 3. $\text{S}(M^*, ID^*, P_{ID^*})$ has never been queried during the Sign Queries.

Definition 3. *A certificateless signature scheme is existentially unforgeable against Type I adversary under adaptively chosen-message attacks iff the probability of success of any polynomially bounded Type I adversary in the above game is negligible.*

Game 2 (for Type II Adversary)

- Setup: \mathcal{C} runs the Setup algorithm, takes as input a security parameter l to obtain the system parameter list params and also the system's master-key. \mathcal{C} then sends params and master-key to the adversary \mathcal{A}_{II} .
- Public-Key Queries $\text{PK}(ID_i)$: \mathcal{A}_{II} can request a user's (whose identity is ID_i) public key. On receiving a query $\text{PK}(ID_i)$, \mathcal{C} replies the public key P_i .
- Private-Key Queries $\text{Pr}(ID_i)$: \mathcal{A}_{II} can request the private key of a user with identity ID_i . In respond, \mathcal{C} outputs the private key S_i .
- Sign Queries $\text{S}(M, ID_i, P_i)$: \mathcal{A}_{II} can request a user's (whose identity is ID_i) signature on a message M . On receiving a query $\text{S}(M, ID_i, P_i)$, \mathcal{C} replies with a signature σ on message M for the user with identity ID_i under public key P_i .
- Output: This procedure contains three steps.

Step 1: Select target identity: \mathcal{A}_{II} selects a target identity ID^* whose public key has been asked during Public-Key Queries. He Submits (ID^*, P_{ID^*}) to \mathcal{C} .

Step 2: Further queries: \mathcal{A}_{II} can make more Public-Key, Private-Key and Sign Queries.

Step 3: Forge: \mathcal{A}_{II} outputs a tuple $(M^*, \sigma^*, ID^*, P_{ID^*})$. This tuple must satisfy the following requirements:

 1. This signature is a valid one, i.e. it passes the verification algorithm with respect to the identity ID^* under the public key P_{ID^*} .
 2. \mathcal{A}_{II} has never asked the private key of the user with identity ID^* .
 3. $\text{S}(M^*, ID^*, P_{ID^*})$ has never been queried during the Sign Queries.

Definition 4. A certificateless signature scheme is existentially unforgeable against Type II adversary under adaptively chosen-message attacks iff the probability of success of any polynomially bounded Type II adversary in the above game is negligible.

Definition 5. A certificateless signature scheme is existentially unforgeable under adaptively chosen-message attacks iff it is existentially unforgeable against both types of adversaries.

3 Our Scheme

In this section, we present an efficient certificateless signature scheme. The construction is as follows.

- **Setup:** When input a security parameter l , this algorithm runs as follows.
 1. Run \mathcal{IG} on input 1^l to generate (p, G_1, G_2, e, P) , set $g = e(P, P)$.
 2. Choose a random master-key $s \in Z_p^*$ and set $P_0 = sP$.
 3. Choose cryptographic hash functions $H_1 : \{0, 1\}^* \rightarrow Z_p^*$ and $H_2 : \{0, 1\}^n \times G_2 \times G_2 \times G_2 \rightarrow Z_p^*$, where n denote the bit-length of plain-texts.

The system parameters $\text{params} = (G_1, G_2, e, n, P, P_0, g, H_1, H_2)$. The master-key is $s \in Z_p^*$. The message space is $\mathcal{M} = \{0, 1\}^n$.

- **Partial-Private-Key-Extract [20]:** This algorithm accepts an identity $ID_i \in \{0, 1\}^*$ of a user and generates the partial private key for the user as follows.
 1. Compute $y_i = H_1(ID_i)$.
 2. Output the partial private key $D_i = \frac{1}{s+y_i}P$.
- **Set-Secret-Value:** This algorithm takes as input params and a user's identity ID_i . It selects a random $x_i \in Z_p^*$ and outputs x_i as the user's secret value.
- **Set-Private-Key:** This algorithm takes as input params , a user's identity ID_i , the user's partial private key D_i and secret value $x_i \in Z_p^*$. The output of the algorithm is the private key $S_i = (x_i, D_i)$.
- **Set-Public-Key:** This algorithm accepts params , a user's identity ID_i and secret value $x_i \in Z_p^*$ to produce the user's public key $P_i = g^{x_i}$.
- **Sign:** To sign a message $M \in \mathcal{M}$ using the private key S_i , a signer with identity ID_i and corresponding public key P_i , performs the following steps.
 1. Select random $r_1, r_2 \in Z_p^*$.
 2. Compute $R = g^{r_1}, R' = g^{r_2}$, set $v = H_2(M, R, R', P_i)$.
 3. Compute $U = (x_i v + r_1)D_i, w = x_i v + r_2$.
 4. Output (U, v, w) as the signature on M .
- **Verify:** To verify a signature (U, v, w) on a message M for an identity ID_i under public key P_i , the verifier performs the following steps.
 1. Compute $R = e(U, P_0 + H_1(ID_i)P)P_i^{-v}, R' = g^w P_i^{-v}$.
 2. Verify $v \stackrel{?}{=} H_2(M, R, R', P_i)$ holds with equality.
 If it does, output true. Otherwise, output \perp .

4 Security Proof

Assuming that the q -SDH problem in G_1 and DL problems in both G_1 and G_2 are hard, we now prove the security of the above signature scheme.

Theorem 1. *Our scheme is unforgeable against type I adversary in the random oracle model assuming the q -SDH problem in G_1 is intractable.*

Proof. Let \mathcal{C} be a q -SDH problem attacker, \mathcal{A} is a type I adversary who interacts with \mathcal{C} following Game 1. We take hash functions H_1 and H_2 as random oracles. Assume that \mathcal{A} 's target identity is ID^* , and he can forge a valid signature on a message M^* for the identity ID^* .

\mathcal{C} is given $(P, \alpha P, \alpha^2 P, \dots, \alpha^q P)$ as an input to the q -SDH problem and aims to find a pair $(c, \frac{1}{\alpha+c} P)$. In Setup phase, it selects a generator $P' \in G_1$ such that it knows $q - 1$ pairs $(h_i, \frac{1}{\alpha+h_i} P')$ for random $h_1, \dots, h_{q-1} \in Z_p^*$. To do so,

1. It picks random $h_1, \dots, h_{q-1} \in Z_p^*$ and expands $f(z) = \prod_{i=1}^{q-1} (z+h_i)$ to obtain $c_0, \dots, c_{q-1} \in Z_p^*$ so that $f(z) = \sum_{i=0}^{q-1} c_i z^i$.
2. It sets $P' = \sum_{i=0}^{q-1} c_i (\alpha^i P) = f(\alpha)P$, the public key P'_0 is fixed to $P'_0 = \sum_{i=1}^q c_{i-1} (\alpha^i P) = \alpha P'$ although \mathcal{C} does not know α .
3. For $1 \leq i \leq q - 1$, \mathcal{C} expands $f_i(z) = f(z)/(z + h_i) = \sum_{i=0}^{q-2} d_i z^i$ and gets $\sum_{i=0}^{q-2} d_i (\alpha^i P) = f_i(\alpha)P = \frac{f(\alpha)}{\alpha+h_i} P = \frac{1}{\alpha+h_i} P'$. The pairs $(h_i, \frac{1}{\alpha+h_i} P')$ are computed.

We let $g' = e(P', P')$, the params given to \mathcal{A} is $(G_1, G_2, e, n, P', P'_0, g', H_1, H_2)$, which has the correct distribution.

H₁ queries: For simplicity, we assume that the queries to H_1 are distinct. When \mathcal{A} issues a query ID_i to H_1 , \mathcal{C} replies h_i which is previously selected and increments i . At some point, \mathcal{A} uniformly chooses an identity ID^* and submits it to \mathcal{C} . In response, \mathcal{C} replies $c \in Z_p^*$ which is randomly selected.

H₂ queries: It can be naturally simulated. Namely, whenever \mathcal{A} issues a query (M_i, R_i, R'_i, P_i) to H_2 , \mathcal{C} picks $v_i \in Z_p^*$ at random and returns v_i as answer.

Partial-Private-Key Queries: \mathcal{C} maintains a initially empty list K^{list} . When \mathcal{A} issues a query PPK(ID^*), \mathcal{C} aborts. While \mathcal{A} issues a query PPK(ID_i) where $ID_i \in \{ID_1, \dots, ID_{q-1}\}$, the same answer from K^{list} will be given if the request has been asked before; otherwise, \mathcal{C} does as follows

1. If there's a tuple (ID_i, D_i, x_i, P_i) which is indexed by ID_i is found on K^{list} , then \mathcal{C} sets $D_i = \frac{1}{\alpha+h_i} P'$ which is previously computed, returns D_i as answer.
2. Otherwise, \mathcal{C} sets $D_i = \frac{1}{\alpha+h_i} P'$ which is previously computed, returns D_i as answer and adds (ID_i, D_i, x_i, P_i) to K^{list} .

Public-Key Queries: When \mathcal{A} issues a query PK(ID) where $ID \in \{ID_1, \dots, ID_{q-1}, ID^*\}$, the current public key relates to ID from K^{list} will be given if the request has been asked before; otherwise, \mathcal{C} does as follows

1. If the query is on ID^* , when there's a tuple (ID^*, D^*, x^*, P^*) which is indexed by ID^* is found on K^{list} , \mathcal{C} selects a random $x^* \in Z_p^*$, sets the public key $P^* = g^{x^*}$, returns P^* as answer and updates (ID^*, D^*, x^*, P^*) to the new value; while no such a tuple matches, \mathcal{C} sets $D^* = \perp$, selects a random $x^* \in Z_p^*$, computes the public key $P^* = g^{x^*}$, returns P^* as answer and adds (ID^*, D^*, x^*, P^*) to K^{list} .
2. Otherwise, the query is on $ID_i \in \{ID_1, \dots, ID_{q-1}\}$. When there's a tuple (ID_i, D_i, x_i, P_i) which is indexed by ID_i is found on K^{list} , \mathcal{C} selects a random $x_i \in Z_p^*$, sets the public key $P_i = g^{x_i}$, returns P_i as answer and updates (ID_i, D_i, x_i, P_i) to the new value; while no such a tuple matches, \mathcal{C} selects a random $x_i \in Z_p^*$, computes the public key $P_i = g^{x_i}$, returns P_i as answer and adds (ID_i, D_i, x_i, P_i) to K^{list} .

Private-Key Queries: When \mathcal{A} issues a query $\text{Pr}(ID)$ where $ID \in \{ID_1, \dots, ID_{q-1}, ID^*\}$, if $ID = ID^*$, \mathcal{C} aborts; else if \mathcal{A} has ever made an Public-Key-Replacement query on ID , \mathcal{C} returns \perp ; otherwise, \mathcal{C} first makes Partial-Private-Key and Public-Key Queries on ID , if \mathcal{C} does not abort, then returns the private key of the user whose identity is ID .

Public-Key-Replacement Queries: \mathcal{A} can replace any user's public key as stated in Game 1.

On receive a Sign query $S(M, ID, P_{ID})$, where $ID \in \{ID_1, \dots, ID_{q-1}, ID^*\}$ and P_{ID} denotes the current public key of the user whose identity is ID , \mathcal{C} creates a signature as follows

1. Pick $U_* \in G_1$, $v_* \in Z_p^*$ and $w_* \in Z_p$ at random.
2. Compute $R_* = e(U_*, P'_0 + H_1(ID)P')$ $P_{ID}^{-v_*}$, $R'_* = g^{w_*} P_{ID}^{-v_*}$.
3. Set $H_2(M, R_*, R'_*, P_{ID}) = v_*$.
4. Return $(M, \sigma = (U_*, v_*, w_*), ID, P_{ID})$ as answer.

Note that \mathcal{A} (everyone) can verify $\sigma = (U_*, v_*, w_*)$ is a valid signature on message M for identity ID under public key P_{ID} .

The next step of the simulation is to apply the 'forking' technique formalized in [14]: Let ID^* is the target identity that \mathcal{A} has chosen. Suppose $(M^*, (U, v, w), ID^*, P_{ID^*})$ be a forgery that output by \mathcal{A} at the end of the attack. Note that if \mathcal{A} does not output ID^* as a part of the forgery, \mathcal{C} just aborts the simulation. \mathcal{C} then replays \mathcal{A} with the same random tape but different choice of the hash function H'_2 to get another forgery $(M^*, (U', v', w'), ID^*, P_{ID^*})$. From these two forgeries, \mathcal{C} obtains

$$R = e(U, P'_0 + cP')P_{ID^*}^{-v}, R' = g^{w'} P_{ID^*}^{-v}$$

and

$$R = e(U', P'_0 + cP')P_{ID^*}^{-v'}, R' = g^{w'} P_{ID^*}^{-v'}$$

Since (U, v, w) and (U', v', w') are valid signatures on M^* , \mathcal{C} consequently obtains the following (Here we let $P_{ID^*} = g^a$):

$$\begin{aligned} g'^w P_{ID^*}^{-v} &= g'^{w'} P_{ID^*}^{-v'} \\ g'^w g'^{-av} &= g'^{w'} g'^{-av'} \\ g'^a &= g'^{(v-v')^{-1}(w-w')} \end{aligned}$$

Since \mathcal{C} has the knowledge of (v, v', w, w') , he can compute $a = (v-v')^{-1}(w-w')$. \mathcal{C} also obtains the following:

$$\begin{aligned} e(U, (\alpha + c)P')P_{ID^*}^{-v} &= e(U', (\alpha + c)P')P_{ID^*}^{-v'} \\ e(U, (\alpha + c)P')e(P', P')^{-av} &= e(U', (\alpha + c)P')e(P', P')^{-av'} \\ e((\alpha + c)U - avP', P') &= e((\alpha + c)U' - av'P', P') \end{aligned}$$

From the last equation, \mathcal{C} has the following

$$\begin{aligned} (\alpha + c)U - avP' &= (\alpha + c)U' - av'P' \\ (\alpha + c)(U - U') &= a(v - v')P' \end{aligned}$$

Since \mathcal{C} has the knowledge of (v, v', a, U, U') , he can compute

$$\frac{1}{\alpha + c}P' = a^{-1}(v - v')^{-1}(U - U')$$

From $\frac{1}{\alpha+c}P'$, \mathcal{C} can proceed as in [24] to extract $\frac{1}{\alpha+c}P$: It first obtains $\gamma_{-1}, \gamma_0, \dots, \gamma_{q-2} \in Z_p^*$ for which $f(z)/(z+h) = \gamma_{-1}/(z+h) + \sum_{i=0}^{q-2} \gamma_i z^i$ and eventually computes

$$\frac{1}{\alpha + c}P = \frac{1}{\gamma_{-1}} \left[\frac{1}{\alpha + c}P' - \sum_{i=0}^{q-2} \gamma_i \alpha^i P \right]$$

So \mathcal{C} has successfully obtains the solution of q -SDH problem. By now, we obtain a contradiction and hence, complete the proof.

Theorem 2. *Our scheme is existentially unforgeable against the type II adversary in the random oracle model assuming the DL problem is intractable.*

Proof. Let \mathcal{A} be our type II adversary. \mathcal{A} has access to the master-key, but cannot perform any public key replacement. \mathcal{C} is given an instance (g, g^a) of the DL problem in G_2 . We will show how can \mathcal{C} solve the DL problem (i.e. to compute a) using \mathcal{A} 's capability as follows.

Firstly, \mathcal{C} generates the KGC's master-key $s \in Z_p^*$ and the system parameters $\text{params}=(G_1, G_2, e, n, P, P_0, g, H_1, H_2)$. Then \mathcal{A} is provided with params and the master-key s . Since \mathcal{A} has access to the master-key, he can do Partial-Private-Key-Extract himself.

Suppose that \mathcal{A} can forge a valid signature on message M^* for identity ID^* under public key P_{ID^*} . \mathcal{C} sets ID^* 's public key as $P_{ID^*} = g^a$ for some unknown a . When \mathcal{A} issues an H_1 query on ID_i , \mathcal{C} picks a random $h_i \in Z_p^*$ and returns as answer. While for an H_2 query on (M_i, R_i, R'_i, P_i) , \mathcal{C} picks a random $v_i \in Z_p^*$ and returns as answer. When \mathcal{A} issues a public key query on an identity $ID_i \neq ID^*$,

\mathcal{C} picks a random $x_i \in Z_p^*$ as ID_i 's secret value, computes $P_i = g^{x_i}$, returns P_i as answer and adds the tuple (ID_i, D_i, x_i, P_i) to K^{list} which is initially empty (where $D_i = \frac{1}{s+H_1(ID_i)}P$); otherwise, returns $P_{ID^*} = g^a$. Whenever \mathcal{A} submits a private key query on ID_i , if $ID_i = ID^*$, \mathcal{C} aborts; otherwise $ID_i \neq ID^*$, if the query $PK(ID_i)$ has not been queried, he first makes $PK(ID_i)$, eventually returns (x_i, D_i) as answer. To answer a Sign query, \mathcal{C} replies with a valid signature if the query is not $S(M^*, ID^*, P_{ID^*})$ (the simulation is the same as mentioned in the proof process of Theorem 1); otherwise, he aborts. Suppose \mathcal{A} eventually outputs a valid signature (U, v, w) on message M^* under identity ID^* and public key P_{ID^*} . Applying the forking technique, a set of two forged signatures (U, v, w) and (U', v', w') on the same message M^* for identity ID^* under public key P_{ID^*} will be obtained. When this happens, \mathcal{C} gets

$$R = e(U, P_0 + H_1(ID^*)P)P_{ID^*}^{-v}, R' = g^w P_{ID^*}^{-v}$$

and

$$R = e(U', P_0 + H_1(ID^*)P)P_{ID^*}^{-v'}, R' = g^{w'} P_{ID^*}^{-v'}$$

Since (U, v, w) and (U', v', w') are valid signatures on M^* , \mathcal{C} consequently obtains the following

$$\begin{aligned} g^w P_{ID^*}^{-v} &= g^{w'} P_{ID^*}^{-v'} \\ g^w g^{-av} &= g^{w'} g^{-av'} \\ g^a &= g^{(v-v')^{-1}(w-w')} \end{aligned}$$

Because \mathcal{C} has the knowledge of (v, v', w, w') , he can compute $a = (v - v')^{-1}(w - w')$. And hence, \mathcal{C} has successfully obtains the solution of DL problem.

5 Efficiency

Table 1 gives a comparison of computational efforts required for our scheme with that of the signature schemes in [7,9,10,17,21] in the Sign and Verify algorithms. Here we only consider the costly operations which defined below, and we omit the computational effort of the hash operation $H(ID)$ in the Sign algorithm, since it can be computed only once.

Table 1. Comparison of Computational Efforts

| Schemes | Sign | Verify |
|----------------|-----------|----------------|
| Scheme in [7] | $2S$ | $3P + 1S + 1H$ |
| Scheme in [9] | $2P + 3S$ | $4P + 1H + 1E$ |
| Scheme in [10] | $2S + 1H$ | $4P + 1S + 2H$ |
| Scheme in [17] | $2S$ | $2P + 1S + 1H$ |
| Scheme in [21] | $3S + 2H$ | $4P + 3H$ |
| Our Scheme | $1S + 2E$ | $1P + 1S + 2E$ |

P : Pairing Operation S : Scalar Multiplication in G_1
 H : MapToPoint Hash E : Exponentiation in G_2

Our Sign algorithm requires no pairing operation and two exponentiation operations in G_2 . Our Verify algorithm requires only one pairing operation, much less than it is required in the Verify algorithms of the other schemes [7,9,10,17,21].

6 Conclusion

It is interesting to investigate secure and efficient certificateless signature schemes. In this paper, we have proposed a secure certificateless signature scheme. The scheme is constructed from bilinear maps. An advantage of our new scheme over the other existing certificateless signature schemes is its efficiency in computation. The total number of pairing operations in the signing and verification processes of our new scheme is one. This is probably the best to achieve in pairing based signature schemes. The proofs of the existential unforgeability of our new scheme under adaptively chosen message attack for both types of adversaries are given as well.

References

1. Al-Riyami, S., Paterson, K.: Certificateless public key cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003)
2. Barreto, P., Libert, B., McCullagh, N., Quisquater, J.: Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 515–532. Springer, Heidelberg (2005)
3. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: ACM CCCS 1993, pp. 62–73 (1993)
4. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004)
5. Boneh, D., Franklin, F.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
6. Cao, X., Paterson, K., Kou, W.: An attack on a certificateless signature scheme, Cryptology ePrint Archive, Report 2006/367 (2006)
7. Gorantla, M., Saxena, A.: An efficient certificateless signature scheme. In: Hao, Y., Liu, J., Wang, Y.-P., Cheung, Y.-m., Yin, H., Jiao, L., Ma, J., Jiao, Y.-C. (eds.) CIS 2005. LNCS (LNAI), vol. 3802, pp. 110–116. Springer, Heidelberg (2005)
8. Hu, B., Wong, D., Zhang, Z., Deng, X.: Key replacement attack against a generic construction of certificateless signature. In: Batten, L.M., Safavi-Naini, R. (eds.) ACISP 2006. LNCS, vol. 4058, pp. 235–346. Springer, Heidelberg (2006)
9. Huang, X., Susilo, W., Mu, Y., Zhang, F.: On the security of a certificateless signature scheme. In: Desmedt, Y.G., Wang, H., Mu, Y., Li, Y. (eds.) CANS 2005. LNCS, vol. 3810, pp. 13–25. Springer, Heidelberg (2005)
10. Li, X., Chen, K., Sun, L.: Certificateless signature and proxy signature schemes from bilinear pairings. Lithuanian Mathematical Journal 45, 76–83 (2005)
11. Libert, B., Quisquater, J.: On constructing certificateless cryptosystems from identity based encryption. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 474–490. Springer, Heidelberg (2006)

12. Mu, Y., Susilo, W.: Identity-based instantaneous broadcast system in mobile ad-hoc networks. In: The 2004 International Workshop on Mobile Systems, E-commerce and Agent Technology, USA, pp. 35–40 (2004)
13. Park, J.: An attack on the certificateless signature scheme from EUC Workshops 2006, Cryptology ePrint Archive, Report 2006/442 (2006)
14. Pointcheval, D., Stern, J.: Security proofs for signature schemes. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 387–398. Springer, Heidelberg (1996)
15. Shamir, A.: Identity based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
16. Susilo, W., Zhang, F., Mu, Y.: Identity-based strong designated verifier signature schemes. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 313–324. Springer, Heidelberg (2004)
17. Yap, W., Heng, S., Goi, B.: An efficient certificateless signature scheme. In: Zhou, X., Sokolsky, O., Yan, L., Jung, E.-S., Shao, Z., Mu, Y., Lee, D.C., Kim, D., Jeong, Y.-S., Xu, C.-Z. (eds.) EUC Workshops 2006. LNCS, vol. 4097, pp. 322–331. Springer, Heidelberg (2006)
18. Yum, D., Lee, P.: Generic construction of certificateless signature. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 200–211. Springer, Heidelberg (2004)
19. Zhang, Z., Feng, D.: Key replacement attack on a certificateless signature scheme. Cryptology ePrint Archive, Report 2006/453 (2006)
20. Zhang, F., Safavi-Naini, R., Susilo, W.: An efficient signature scheme from bilinear pairings and its applications. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 277–290. Springer, Heidelberg (2004)
21. Zhang, Z., Wong, D., Xu, J., Feng, D.: Certificateless public-key signature: security model and efficient construction. In: Zhou, J., Yung, M., Bao, F. (eds.) ACNS 2006. LNCS, vol. 3989, pp. 293–308. Springer, Heidelberg (2006)

A Practical Identity-Based Signature Scheme from Bilinear Map^{*}

Zhu Wang¹ and Huiyan Chen²

¹ State Key Laboratory of Information Security Graduate School of Chinese Academy of Sciences, Beijing, 100049

² Beijing Electronic Science and Technology Institute, Beijing 100070
chenhy2003@gmail.com

Abstract. In this paper, we present a new identity-based signature scheme with message recovery based on bilinear map. Our scheme is proved secure against existential forgery on adaptive chosen message and ID attack under the random oracle model. This new scheme shortens the total length of the original message and the appended signature and adapts to the ubiquitous network scenario very well.

Keywords: Identity-based signature, bilinear map, ID reduction, message recovery.

1 Introduction

In ubiquitous computing, the bandwidth of ubiquitous network is usually constrained, so it is desirable to shorten the total length of the original message M and the appended signature x . In this research area, there are two kinds of ideas adopted: one which is to directly produce short signature for message M , the other which is to “fold” part of message into the signature in such a way that it is “recoverable” by the verifier (i.e, signature scheme has the partial message recovery property). The former is taken by schemes proposed by D. Boneh et al. [10], F. Zhang et al. [11], D. Boneh and X. Boyen [12] and so on. In this paper, we mainly focus on the latter. On the whole, the existing digital signatures with message recovery may be classified into two types: RSA-based schemes and discrete-logarithm-based schemes. PSS-R [3] and ISO/IEC 9796-1,9796-2 are signature schemes with message recovery in the RSA type. The Nyberg-Rueppel [4,5,6], Miyaji [7] and Okamoto et al. [9] schemes are in DL (discrete logarithm) type.

The concept of identity-based cryptography was proposed in 1984 by Shamir [14]. The idea behind identity-based cryptography is that the user’s public key can be derived from arbitrary string (e-mail address, IP address combined to a user name, social security number,...) which identifies him in a non ambiguous way. This greatly reduces the problems with key management. This kind of system needs trusted authority called private key generator (PKG) whose task

^{*} This work is supported by the National Natural Science Foundation of China (No. 60577039).

is to compute user's private key from user's identity information (users do not generate their key pairs themselves). Several practical identity-based signature schemes [1,2,13] have been devised since 1984, but no identity-based signature scheme with message recovery goes out into the world until the scheme proposed by F. Zhang et al. [15] in 2005. F. Zhang et al. didn't quantify the security of their signature schemes in [15]. In addition, there are some problems occur in F. Zhang et al.'s schemes (see section 3).

In this paper, we present a new identity-based signature scheme with message recovery based on bilinear map, referred to as IDSMR. Its security is based on Computational Diffie-Hellman Assumption, CDH for short. IDSMR can deal with any message with arbitrary length.

Signature schemes from three message identification schemes such as Fiat-Shamir [1] are a typical class of practical signature schemes. To prove the security of such a class of signature schemes, K. Ohta and T. Okamoto presented a new key technique "ID reduction", in which the identification scheme corresponding to the signature scheme was used. In [8], K. Ohta and T. Okamoto thought that ID reduction technique had advantage over the previous technique, "forking lemma", by Pointcheval and Stern [16], and partly owed the advantage of ID reduction technique over forking lemma to the case that analyzing the identification scheme corresponding to the signature scheme was easier than analyzing the signature scheme. To prove that IDSMR is existentially unforgeable against adaptive chosen message and ID attack under the random oracle model, we make use of the ID reduction Technique and the results in [8,9].

The paper will proceed as follows. In section 2, we review some preliminaries used throughout this paper. In section 3, we review and analyse F. Zhang et al.'s schemes. In section 4, we present our signature scheme with message recovery. In section 5, we give security analysis of IDSMR. In section 6, we compare our scheme with other schemes. Section 7 concludes this paper.

2 Preliminaries

2.1 Notations

Throughout this paper, we will use the following notations. $|q|$ denotes the length of q in bit. If $|q| = 0$, q is denoted as \emptyset . Z^+ denotes the set of natural numbers and $\{0, 1\}^*$ denotes the space of finite binary strings. Let $[m]^{l_1}$ denote the most significant l_1 bits of m and $[m]_{l_2}$ denote the least significant l_2 bits of m . We denote by $a||b$ the string which is the concatenation of strings a and b . We also denote $[x]=y$ if $y \leq x < y+1$ and $y \in Z^+$. $a \oplus b$ denotes the bitwise XOR of bit strings a and b . If G is a group and $P \in G$, $(P)_2$ denotes the binary string representation of P .

2.2 Bilinear Map

Let G_1 be a cyclic additive group, whose order is a prime p , and G_2 be a cyclic multiplicative group with the same order p . Let $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a bilinear map with the following properties:

- (1) Bilinearity: $\widehat{e}(aP, bQ) = \widehat{e}(P, Q)^{ab}$ for all $P, Q \in G_1, a, b \in Z_p$
- (2) Non-degeneracy: There exists $P, Q \in G_1$ such that $\widehat{e}(P, Q) \neq 1$, in other words, the map does not send all pairs in $G_1 \times G_1$ to the identity in G_2 ;
- (3) Computability: There is an efficient algorithm to compute $\widehat{e}(P, Q)$ for all $P, Q \in G_1$.

The Weil and Tate pairings associated with supersingular elliptic curves can be modified to create such bilinear maps.

Definition 1. *CDH:* Let G_1 be a cyclic additive group generated by P , whose order is a prime p . For $a, b \in Z_p$, given P, aP, bP , compute abP . An algorithm A has advantage ϵ in solving CDH in G_1 if

$$Pr[A(P, aP, bP)=abP] \geq \epsilon$$

where the probability is over the random choice of generator $P \in G_1$, the random choice of $a, b \in Z_p^*$ and the random bits consumed by A .

Definition 2. We say that the (t, ϵ) -CDH assumption holds in G_1 if no t -time algorithm has advantage at least ϵ in solving CDH in G_1 .

3 Analysis of F. Zhang et al.’s Scheme

Zhang et al. proposed two schemes in [15]: an ID-based message recovery signature scheme for messages of fixed length, and an ID-based partial message recovery signature scheme for messages of arbitrary length. Here we review their scheme for messages of fixed length and analyze its problems.

- **Setup:** The private key generator(PKG) chooses a random number $s \in Z_p^*$ and sets $P_{pub} = sP$. PKG also publishes system parameters $\{G_1, G_2, \widehat{e}, p, \lambda, P, P_{pub}, H_1, H_2, F_1, F_2, k_1, k_2\}$, and keeps s as the master-key, which is known only by itself. Here $|p|=k_1+k_2, H_1 : \{0, 1\}^* \rightarrow Z_p^*, H_2 : \{0, 1\}^* \rightarrow G_1^*, F_1 : \{0, 1\}^{k_2} \rightarrow \{0, 1\}^{k_1}, F_2 : \{0, 1\}^{k_1} \rightarrow \{0, 1\}^{k_2}$ are four cryptographic hash functions
- **Extract:** A user submits his/her identity information ID to PKG. PKG computes the user’s public key as $Q_{ID}=H_2(ID)$, and returns $S_{ID}=sQ_{ID}$ to the user as his/her private key.
- **Sign:** Let the message be $m \in \{0, 1\}^{k_2}$
 1. Randomly choose $k \in Z_p^*$, and compute $v=\widehat{e}(P, P)^k$.
 2. Compute $f = F_1(m) || (F_2(F_1(m)) \oplus m)$.
 3. Compute $r = H_1(v) + f \text{ mod } p$
 4. Compute $U = kP - rS_{ID_A}$.

The signature is (r, U) .

- **Verify:** Given ID_A , a message m , and a signature (r, U) , compute

$$r - H_1(\widehat{e}(U, P)\widehat{e}(Q_{ID_A}, P_{pub})^r) = f$$

and

$$m = [f]_{k_2} \oplus F_2([f]^{k_1})$$

Check whether $[f]^{k_1} = F_1(m)$ holds. If it is correct, then accept this signature and output true. Otherwise, output \perp .

In the above scheme, if $f \in Z_p$ and $|f| < |p|$, then, in the verification phase, we need padding $(|p| - |f|)0$ s in the left of the binary string representation of f . Otherwise, the signature will be rejected. If $f > p$ and $|f| = |p|$, we say $f = p + f'$ then, in the verification phase, we get

$$r - H_1(\widehat{e}(U, P)\widehat{e}(Q_{IDA}, P_{pub})^r) = f' \text{ and } m = [f']_{k_2} \oplus F_2([f']^{k_1})$$

With a large probability $[f']^{k_1} \neq F_1(m)$, so the signature will be rejected, although it is generated correctly. Zhang et al.'s second scheme for partial message recovery in [15] also suffers the similar problems.

In addition, their two schemes can't seem to deal with the message whose length in bits is less than some fixed length.

4 IDSMR Scheme

This section introduces our signature scheme with message recovery. It works as follows.

- **Setup:** Given a security parameter $l \in Z^+$, the private key generator(PKG) chooses two groups G_1 and G_2 of prime order p (here, $l=|p|$), a generator P of G_1 , a bilinear map $\widehat{e} : G_1 \times G_1 \rightarrow G_2$. Then PKG picks a master-key $s \in Z_p^*$ and computes $P_{pub} = sP$ and $w = \widehat{e}(P, P)$. PKG also chooses cryptographic hash functions $H_1 : \{0, 1\}^* \rightarrow G_1$, $H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^l$, $F_1 : \{0, 1\}^{[l/2]} \rightarrow \{0, 1\}^{[(l+1)/2]}$, $F_2 : \{0, 1\}^{[(l+1)/2]} \rightarrow \{0, 1\}^{[l/2]}$. The system's public parameters are

$$Param = \{p, G_1, G_2, \widehat{e}, P, P_{pub}, w, H_1, H_2, F_1, F_2\}$$

- **Extract:** for an identity ID , the private key is $d_{ID} = sQ_{ID} = sH_1(ID)$.
- **Sign:** To sign a message $m = m_1 || m_2$ (If $|m| = [l/2]$, $m_2 = m$, $m_1 = \emptyset$; if $|m| > [l/2]$, $m_1 = [m]^{|m| - [l/2]}$, $m_2 = [m]_{[l/2]}$;), Alice follows the steps below
 1. Randomly choose $x \in Z_p^*$, and compute $\tau = w^x$.
 2. Compute $f = F_1(m_2) || (F_2(F_1(m_2)) \oplus m_2)$.
 3. Compute $r = [(\tau)_2]_l \oplus f$
 4. Compute $r_0 = H_2(r || m_1)$
 5. Compute $S = xP - r_0 d_{IDA}$.
 6. Alice sends $\sigma = (m_1, r, S)$ to verifier Bob.
- **Verify:** When receiving $\sigma = (m_1, r, S)$, Bob follows the steps below.
 1. Compute $r_0 = H_2(r || m_1)$
 2. Compute $\tau = \widehat{e}(S, P)\widehat{e}(Q_{IDA}, P_{pub})^{r_0}$
 3. Compute $f = r \oplus [(\tau)_2]_l$
 4. Compute $m_2 = [f]_{[l/2]} \oplus F_2([f]^{[(l+1)/2]})$
 5. Accept signature if and only if $[f]^{[(l+1)/2]} = F_1(m_2)$.
- **Remark 1:** If $|(\tau)_2| < l$, we need padding 0 in the left of $(\tau)_2$. If $|m| < [l/2]$, we need some redundancy to sign message m . We choose a hash function

$H : \{0, 1\}^* \rightarrow \{0, 1\}^{\lfloor l/2 \rfloor}$ and set $m' = m || H(m)$, then we sign message m' similar to message m'' ($|m''| \geq \lfloor l/2 \rfloor$). We don't discuss it any more here. Throughout this paper, we assume $|m| \geq \lfloor l/2 \rfloor$ if message m need to be signed.

5 Security

In this section we prove the security of our signature scheme in the random oracle model, with CDH assumption. In order to prove the security of our signature scheme with *ID reduction* technique, we need to introduce a non-identity-based signature scheme, referred to as NIDS, and an identification scheme corresponding to NIDS, referred to as IFNIDS.

5.1 Attack Model for Identity-Based Signature Schemes

The most general known notion of security of a non-identity-based signature scheme is existential unforgeability under adaptive chosen message attacks (EUF-ACMA); in this model, an adversary wins the game if he outputs a valid pair of a message and a signature, where he is allowed to ask the signer to sign any message except the output. We consider the following natural generalization of this notion, which is acceptable as a standard model of security for identity-based signature schemes with message recovery.

Definition 3. *An identity-based signature scheme with message recovery, which consists of four algorithms **Setup**, **Extract**, **Sign**, and **Verify** playing the same role as ours, has the existential unforgeability for adaptive chosen message and ID attacks (EUF-ID-ACMA) property if no polynomial time algorithm \mathcal{A} has a non-negligible succeed probability in the following game:*

1. Challenger \mathcal{C} runs **Setup** of the scheme. The resulting system parameters are given to \mathcal{A} .
2. \mathcal{A} issues the following queries as he wants:
 - (a) **Hash function query:** \mathcal{C} computes the value of the hash function for the requested input and sends the value to \mathcal{A} .
 - (b) **Extract query:** Given an identity ID , \mathcal{C} returns the private key corresponding to ID which is obtained by running **Extract**.
 - (c) **Sign query:** Given an identity ID and a message m , \mathcal{C} returns a signature which is obtained by running **Sign**.
3. \mathcal{A} outputs (ID, σ, m_1) , where ID is an identity, and σ is a signature of m ($m = m_1 || m_2$). If $|m| > \lfloor l/2 \rfloor$, $m_1 = [m]^{|m| - \lfloor (l+1)/2 \rfloor}$, $m_2 = [m]^{\lfloor l/2 \rfloor}$; if $|m| = \lfloor l/2 \rfloor$, $m_2 = m$, $m_1 = \emptyset$), such that ID and (ID, m) are not equal to the input of any query to **Extract** and **Sign**, respectively. \mathcal{A} wins the game if σ is a valid signature of m for ID .

5.2 NIDS and IFNIDIS

Descriptions of NIDS Scheme. NIDS is described by three algorithms **Keygen**, **Sign** and **Verify**.

–**Keygen:** Given a security parameter $l \in Z^+$, signer \mathcal{S} chooses the same system parameters as PKG of IDSMR except that it chooses its public key Q_{ID} and computes its private key $d_{ID}=sQ_{ID}$, doesn't choose hash function H_1 . The system's public parameters are

$$Param=\{p,G_1,G_2,\hat{e},P,P_{pub},Q_{ID},w,H_2,F_1,F_2\}$$

–**Sign:** To sign a message $m = m_1||m_2$ (If $|m| = [l/2]$, $m_2 = m$, $m_1 = \emptyset$; if $|m| > [l/2]$, $m_1 = [m]^{|m|-[l/2]}$, $m_2 = [m]_{[l/2]}$), \mathcal{S} follows the steps below

1. Randomly choose $x \in Z_p^*$, and compute $\tau=w^x$.
2. Compute $f = F_1(m_2)|| (F_2(F_1(m_2)) \oplus m_2)$.
3. Compute $r = [(\tau)_2]_l \oplus f$
4. Compute $r_0 = H_2(r||m_1)$
5. Compute $S = xP - r_0d_{ID}$.
6. \mathcal{S} sends $\sigma = (m_1, r, S)$ to verifier \mathcal{V} .

–**Verify:** When receiving $\sigma = (m_1, r, S)$, \mathcal{V} follows the steps below:

1. Compute $r_0 = H_2(r||m_1)$
2. Compute $\tau=\hat{e}(S,P)\hat{e}(Q_{ID},P_{pub})^{r_0}$
3. Compute $f = r \oplus [(\tau)_2]_l$
4. Compute $m_2 = [f]_{[l/2]} \oplus F_2([f]^{[(l+1)/2]})$
5. Accept signature if and only if $[f]^{[(l+1)/2]} = F_1(m_2)$.

Descriptions of IFNIDS Scheme. In IFNIDS, prover \mathcal{P} publishes its public system parameters while keeping the corresponding secret key, and proves its identity to verifier \mathcal{V} . Here hash functions F_1, F_2 are shared by \mathcal{P} and \mathcal{V} . IFNIDS works as follows.

–**Keygen:** Given a security parameter $l \in Z^+$, prover \mathcal{P} chooses its public key Q_{ID} , computes its private key $d_{ID}=sQ_{ID}$, chooses the same system parameters as signer \mathcal{S} of NIDS except that it doesn't choose hash function H_2 . The system's public parameters are

$$Param=\{p,G_1,G_2,\hat{e},P,P_{pub},Q_{ID},w,F_1,F_2\}$$

–**Identification Protocol:** \mathcal{P} proves its identity and \mathcal{V} checks the validity of \mathcal{P} ' proof as follows:

- (1) \mathcal{P} chooses message m ($m = m_1||m_2$. If $|m| = [l/2]$, $m_2 = m$, $m_1 = \emptyset$; if $|m| > [l/2]$, $m_1 = [m]^{|m|-[l/2]}$, $m_2 = [m]_{[l/2]}$) and generates r as follows:

$$f = F_1(m_2)|| (F_2(F_1(m_2)) \oplus m_2), \tau = w^x, r = f \oplus [(\tau)_2]_l$$

Here $x \in Z_p^*$ is uniformly selected. \mathcal{P} sends (r, m_1) to verifier \mathcal{V} .

- (2) \mathcal{V} generates random challenge $u \in Z_p^*$ and sends it to \mathcal{P} .
- (3) \mathcal{P} generates an answer S as follows and send it to \mathcal{V} .

$$S = xP - ud_{ID}$$

(4) \mathcal{V} checks the validity of \mathcal{P} ' proof through whether $[f]^{[(l+1)/2]} = F_1(m_2)$ holds or not, where

$$\tau = \widehat{e}(S, P)\widehat{e}(Q_{ID}, P_{pub})^u, f = r \oplus [(\tau)_2]_l, m_2 = [f]_{[l/2]} \oplus F_2([f]^{[(l+1)/2]}).$$

Security of NIDS and IFNIDS. In order to analyze the security of NIDS and IFNIDS, we firstly introduce the following notions similar to those [8,9]. Here we assume all hash functions are modeled as random oracles.

Definition 4. An EUF-ACMA adversary \mathcal{A} breaks NIDS with $(t, q_{sig}, q_{F_1}, q_{F_2}, q_{H_2}, \epsilon)$ if and only if \mathcal{A} queries **Sign** at most q_{sig} times, queries hash functions F_1, F_2, H_2 at most $q_{F_1}, q_{F_2}, q_{H_2}$ times respectively, and can forge a signature of NIDS within time t with success probability greater than ϵ .

Definition 5. NIDS is $(t, q_{sig}, q_{F_1}, q_{F_2}, q_{H_2}, \epsilon)$ -secure if and only if no adversary can not break it with $(t, q_{sig}, q_{F_1}, q_{F_2}, q_{H_2}, \epsilon)$.

Definition 6. An adversary \mathcal{A} breaks IFNIDS with $(t, q_{F_1}, q_{F_2}, \epsilon)$ if and only if \mathcal{A} as a prover queries hash functions F_1, F_2 at most q_{F_1}, q_{F_2} times respectively, and can cheat honest verifier \mathcal{V} within time t with success probability greater than ϵ .

Definition 7. IFNIDS is $(t, q_{F_1}, q_{F_2}, \epsilon)$ -secure if and only if no adversary can not break it with $(t, q_{F_1}, q_{F_2}, \epsilon)$.

Using the ID Reduction Technique and the results in [9], we can straightforwardly obtain the following lemma.

Lemma 1. ID Reduction Lemma

(1) If \mathcal{A} breaks NIDS with $(t, q_{sig}, q_{F_1}, q_{F_2}, q_{H_2}, \epsilon)$, there exists \mathcal{A}_1 which breaks NIDS with $(t', 0, q_{F_1}, q_{F_2}, 1, \epsilon')$, where $\epsilon' = (1/q_{H_2} - q_{sig}/2^l)(\epsilon - 1/2^l)$, and $t' = t +$ (the simulation time of q_{sig} signatures).

(2) If \mathcal{A}_1 breaks NIDS with $(t', 0, q_{F_1}, q_{F_2}, 1, \epsilon')$, there exists \mathcal{A}_2 which breaks IFNIDS with $(t', q_{F_1}, q_{F_2}, \epsilon')$

(3) If \mathcal{A}_2 breaks IFNIDS with $(t', q_{F_1}, q_{F_2}, \epsilon')$, there exists \mathcal{A}_3 which breaks IFNIDS with $(t', 1, 1, \epsilon'')$, Where $\epsilon'' = \frac{\epsilon' - 1/2^{l/2}}{q_{F_1}}$

Theorem 1. Let $\epsilon \geq \frac{5}{p}$. Suppose CDH in G_1 is (t^*, ϵ^*) -secure, then IFNIDS is $(t, 1, 1, \epsilon)$ -secure, where

$$t^* = \frac{6t'}{\epsilon - 2/p} + O(t_{pm}), \epsilon^* = \frac{1}{2}(1 - e^{-1})^2 > \frac{9}{50}, t' = t + O(2t_p + t_e)$$

Here t_{pm} denotes the computation time of point multiplication over additive group G_1 , t_p denotes the computation time of bilinear map, t_e denotes the computation time of exponentiation over G_2 and e is the base of the natural logarithm.

Due to lack of space, the proof of the above theorem is omitted in this version of the paper. The basic idea of proof is to use boolean matrix and heavy row introduced [9] and is similar to that of proof on Lemma 4 in [9].

5.3 Security of IDSMR

In order to analyze security of IDSMR, we introduce the following quantifiable notions.

Definition 8. An EUF-ID-ACMA adversary \mathcal{A} breaks IDSMR with $(t, q_{sig}, q_{H_1}, q_{H_2}, q_{F_1}, q_{F_2}, \epsilon)$ if and only if \mathcal{A} queries **Extract** at most q_E times, queries **Sign** at most q_{sig} times, queries hash functions H_1, H_2, F_1, F_2 at most $q_{H_1}, q_{H_2}, q_{F_1}, q_{F_2}$ times respectively, and can forge a signature of IDSMR within time t with success probability greater than ϵ .

Definition 9. IDSMR is $(t, q_{sig}, q_{H_1}, q_{H_2}, q_{F_1}, q_{F_2}, \epsilon)$ -secure if and only if no adversary can not break it with $(t, q_{sig}, q_{H_1}, q_{H_2}, q_{F_1}, q_{F_2}, \epsilon)$.

The following theorem shows the relation between IDSMR and NIDS in security.

Theorem 2. In the random oracle model, suppose that an EUF-ID-ACMA adversary \mathcal{A}_0 exists which makes at most q_E **Extract** queries, at most q_{sig} **Sign** queries, and at most q_{H_1} queries to hash function H_1 , and which succeeds within time t_0 of making an existential forgery of IDSMR signature with probability greater than ϵ_0 , then there is an EUF-ACMA adversary \mathcal{A}_1 which succeeds within time $t = O(t_0)$ of making an existential forgery of NIDS signature with probability $\epsilon > \epsilon_0(1 - 1/p)/q_{H_1}$. In addition, the numbers of queries to other hash functions asked by \mathcal{A}_1 are the same as those of \mathcal{A}_0 .

Proof. We show how to construct an EUF-ACMA adversary \mathcal{A}_1 that uses \mathcal{A}_0 to gain advantage $\epsilon_0(1 - 1/p)/q_{H_1}$ against NIDSMR. The game between the challenger and \mathcal{A}_1 starts with the challenger first generating random public system parameters $Param = \{p, G_1, G_2, \hat{e}, P, P_{pub}, Q_{ID}, w, H_2, F_1, F_2\}$ (Here $P_{pub} = sP, Q_{ID} \in G_1$), and a private key $d_{ID} = sQ_{ID}$. The challenger gives $Param$ to algorithm \mathcal{A}_1 . The algorithm \mathcal{A}_1 interacts with \mathcal{A}_0 as follows and maintains list L_1 that is initially empty and is used to keep track of answers to queries asked by \mathcal{A}_0 to oracle H_1 , and challenger maintains lists L_2, L_3 and L_4 that are initially empty and are used to keep track of answers to queries asked by \mathcal{A}_0 to oracle H_2, F_1 and F_2 .

–**Setup:** The algorithm \mathcal{A}_1 gives the algorithm \mathcal{A}_0 the system parameters $\{p, G_1, G_2, \hat{e}, P, P_{pub}, w, H_1, H_2, F_1, F_2\}$ of IDSMR scheme. Here $p, G_1, G_2, \hat{e}, P, P_{pub}, w, H_2, F_1, F_2$ are taken from $Param$.

– **H_1 queries:** When \mathcal{A}_0 asks queries on the hash values of identities, \mathcal{A}_1 checks the list L_1 . If an entry for the query is found, the same answer will be given to \mathcal{A} ; otherwise, a value d_j from Z_p^* will be randomly chosen and d_jP will be used as the answer, (ID_j, d_jP) will then be stored in the list L_1 . The only exception is that \mathcal{A}_1 has to randomly choose one of the H_1 queries from \mathcal{A}_0 , say the i^{th} query, and answers $H_1(ID_i) = Q_{ID}$ for this query.

Note that we assume that \mathcal{A}_0 must ask for $H_1(ID)$ before ID is used in any **Sign** and **Extract** queries.

- **H_2, F_1 and F_2 queries:** When \mathcal{A}_0 asks queries on these hash functions, \mathcal{A}_1 relays these queries to Challenger. Challenger checks the corresponding list. If an entry for the query is found, the same answer will be given to \mathcal{A}_1 ; otherwise, a randomly generated value will be used as an answer to \mathcal{A}_1 , the query and the answer will then be stored in the list. \mathcal{A}_1 relays challenger's responses to \mathcal{A}_0 .
- **Key extraction queries:** When \mathcal{A}_0 asks a private key extraction to ID_j , if $j = i$, then \mathcal{A}_1 fails and stops. If $j \neq i$, then the list L_1 must contain (ID_j, d_jP) . \mathcal{A}_1 sends (ID_j, d_jP) to challenger and relays this query to challenger. Challenger computes private key $d_{ID_j} = sd_jP$ which corresponds to ID_j , and sends d_{ID_j} to \mathcal{A}_1 . \mathcal{A}_1 relays d_{ID_j} to \mathcal{A}_0 .
- **Sign queries:** Given an identity ID and a message $m(= m_1||m_2)$, \mathcal{A}_1 works as follows.
 - (1) \mathcal{A}_1 gets $Q'_{ID} = H_1(ID)$ by simulation for H_1 .
 - (2) \mathcal{A}_1 sends Q_{ID} to challenger and relays this signature query to challenger.
 - (3) Challenger randomly selects $x \in Z_p^*$, computes $d'_{ID} = sQ'_{ID}$ and $\tau = w^x$, gets the hash values by simulation for H_2, F_1 and F_2 , computes signature $\sigma = (m_1, r, S)$ to the signature query (ID, m) (here $m = m_1||m_2$), and sends σ to \mathcal{A}_1 . \mathcal{A}_1 relays this signature σ to \mathcal{A}_0 .
- \mathcal{A}_0 outputs (ID_{out}, m_1, r, S) , where ID_{out} is an identity, m_1 is part of message m , and (m_1, r, S) is a signature to m , such that ID_{out} and (ID_{out}, m) are not equal to the input of any query to **Extract** and **Sign**, respectively.
- If $ID_{out} = ID_i$ and (ID_{out}, m_1, r, S) is valid, then outputs (ID_{out}, m_1, r, S) . Otherwise output fail.

If algorithm \mathcal{A}_1 does not abort during simulation, algorithm \mathcal{A}_0 's view is identical to its view in the attack, furthermore

$$Pr[(ID_{out}, m_1, r, S) is valid | \mathcal{A}_1 \text{ does not abort}] > \epsilon_0$$

Let \mathcal{E}_1 be the event that algorithm \mathcal{A}_1 does not abort during simulation. Let \mathcal{E}_2 be the event that (ID_{out}, m_1, r, S) is valid. Since H_1 is a random oracle, the probability that the output (ID_{out}, m_1, r, S) of \mathcal{A}_0 is valid without any query of $H_1(ID_{out})$ is negligible. Explicitly,

$$Pr[ID_{out} = ID_j \text{ for some } j, j \leq q_{H_1} | \mathcal{E}_1 \wedge \mathcal{E}_2] \geq 1 - 1/p$$

Since i is independently and randomly chosen, we have

$$Pr[ID_{out} = ID_i | (ID_{out} = ID_j \text{ for some } j, j \leq q_{H_1}) \wedge \mathcal{E}_1 \wedge \mathcal{E}_2] \geq 1/(q_{H_1} - q_E)$$

\mathcal{A}_1 's failure during simulation is caused by \mathcal{A} issuing a private query to ID_i , we have

$$Pr[\mathcal{E}_1] = \left(\frac{q_{H_1}-1}{q_{H_1}}\right)\left(\frac{q_{H_1}-2}{q_{H_1}-1}\right) \dots \left(\frac{q_{H_1}-q_E}{q_{H_1}-q_E+1}\right) = \frac{q_{H_1}-q_E}{q_{H_1}}$$

Therefore, we have

$$Pr[(ID_{out} = ID_i) \wedge ((ID_{out}, m_1, r, S) \text{ is valid}) \wedge \mathcal{E}_1] > \epsilon_0(1 - 1/p)/q_{H_1}$$

Combing theorem 9 and 12 and lemma 8, we have

Theorem 3. (Security of IDSMR) Let $\epsilon \geq q_{H_1} \times \frac{p}{p-1} \times ((\frac{5q_{F_1}}{p} + \frac{1}{2^{\lfloor l/2 \rfloor}}) / (\frac{1}{q_{H_2}} - \frac{q_{sig}}{2^l}) + \frac{1}{2^l})$. Suppose CDH is (t^*, ϵ^*) -secure, then IDSMR is $(t, q_{sig}, q_{H_1}, q_{H_2}, q_{F_1}, q_{F_2}, \epsilon)$ -secure, where

$$t^* = \frac{6t'}{\epsilon^{-2/p}} + O(t_{pm}) \text{ and } \epsilon^* = \frac{1}{2}(1 - e^{-1})^2 > \frac{9}{50}$$

Here

$$t' = O(t) + O(q_{sig}(t_e + 2t_{pm}) + t_e + 2t_p)$$

$$\epsilon' = \frac{1}{q_{F_1}} ((\frac{p-1}{pq_{H_1}}\epsilon - \frac{1}{2^l})(\frac{1}{q_{H_2}} - \frac{q_{sig}}{2^l}) - \frac{1}{2^{\lfloor l/2 \rfloor}})$$

where t_{pm} denotes the computation time of point multiplication over additive group G_1 , t_p denotes the computation time of bilinear map, t_e denotes the computation time of exponentiation over G_2 and e is the base of the natural logarithm.

6 Comparison of Schemes

In table 1 below, we compare our scheme with schemes [13][15][17][18] in terms of the total length of the original message and the appended signature, and the number of the dominant operations required by them. In table we use mls, exps, and pcs as abbreviations for point multiplications in G_1 , exponentiations in G_2 and computations of bilinear map respectively.

Table 1. Comparison of Schemes

| Schemes | Total Length* | | Efficiency | | | | | |
|---------------------|---------------------|---|------------|------|-----|--------|------|-----|
| | $ m =l/2$ | $ m >l/2$ | Sign | | | Verify | | |
| | | $(m_1 = [m]^{ m -\lfloor l/2 \rfloor})$ | mls | exps | pcs | mls | exps | pcs |
| F. Hess [13] | $ m + p + G_1 $ | $ m + p + G_1 $ | 1 | 1 | 1 | | 1 | 2 |
| Cha-Cheon [17] | $ m + 2 G_1 $ | $ m + 2 G_1 $ | 2 | | | 1 | | 2 |
| Libert et al. [18] | $ m + p + G_1 $ | $ m + p + G_1 $ | 1 | 1 | | 1 | 1 | 1 |
| F. Zhang et al [15] | $ p + G_1 $ | $ m_1 + p + G_1 $ | 2 | 1 | 1 | | 1 | 2 |
| IDSMR | $ p + G_1 $ | $ m_1 + p + G_1 $ | 2 | 1 | | | 1 | 2 |

(*) Total length is the length of the original message and the appended signature.

7 Conclusion

This paper presented a signature scheme with message recovery. It is proved to be secure in the strongest sense (i.e., existentially unforgeable under adaptive chosen message and ID attacks) in the random oracle model under the CDH assumption. Furthermore, our scheme can deal with any message with arbitrary length and shortens the length of the original message and the appended signature by “folding” part of message into the signature.

Acknowledgement

The authors would like to thank anonymous referees for their helpful comments.

References

1. Fiat, A., Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987)
2. Guillou, L., Quisquater, J.-J.: A "Paradoxical" Identity-Based Signature Scheme Resulting From Zero-Knowledge. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 216–231. Springer, Heidelberg (1990)
3. Bellare, M., Rogaway, P.: The Exact Security of Digital Signatures –How to Sign with RSA and Rabin. In: Proc. of Eurocrypt's 1996. LNCS, pp. 399–416. Springer, Heidelberg (1996)
4. Nyberg, K., Rueppel, R.A., New, A.: Signature Scheme Based on the DSA Giving Message Recovery. In: Proc. of the First ACM Conference on Computer and Communications Security (1993)
5. Nyberg, K., Rueppel, R.A.: Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem. In: Proc. of Eurocrypt's 1994. LNCS, pp. 182–193. Springer, Heidelberg (1995)
6. Nyberg, K., Rueppel, R.A.: Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem. *Designs, Codes and Cryptography* 7, 61–81 (1996)
7. Miyaji, A.: A Message Recovery Signature Scheme Equivalent to DSA over Elliptic Curves. In: Proc. of Asiacrypt's 1996. LNCS, pp. 1–14. Springer, Heidelberg (1996)
8. Ohta, K., Okamoto, T.: On the Concrete Security Treatment of Signatures Derived from Identification. In: RobVis 2001. LNCS, pp. 354–369. Springer, Heidelberg (1998)
9. Abe, M., Okamoto, T.: A Signature Scheme with Message Recovery as Secure as Discrete Logarithm. *IEICE Trans. Fundamentals* E84-A(1), 197–204 (2001)
10. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001)
11. Zhang, F., Safavi-Naini, R., Susilo, W.: An Efficient Signature Scheme from Bilinear Pairings and Its Applications. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 277–290. Springer, Heidelberg (2004)
12. Boneh, D., Boyen, X.: Short Signatures Without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004)
13. Hess, F.: Efficient identity based signature schemes based on pairings. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, Springer, Heidelberg (to appear)
14. Shamir, A.: Identity Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, Springer, Heidelberg (1985)
15. Zhang, F., Susilo, W., Mu, Y.: Identity-based Partial Message Recovery Signatures (or How to Shorten ID-based Signatures). In: Patrick, A.S., Yung, M. (eds.) FC 2005. LNCS, vol. 3570, pp. 47–59. Springer, Heidelberg (2005)

16. Pointcheval, D., Stern, J.: Security Proofs for Signature Schemes. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 387–398. Springer, Heidelberg (1996)
17. Cha, J.C., Cheon, J.H.: An identity-based signature from gap Diffie-Hellman groups. In: PKC 2003. LNCS, vol. 2567, pp. 18–30. Springer, Heidelberg (2003)
18. Barreto, P.S.L.M., Libert, B., McCullagh, N., Quisquater, J.-J.: Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 515–532. Springer, Heidelberg (2005)

Linkable Ring Signatures from Linear Feedback Shift Register^{*}

Dong Zheng^{1,3}, Xiangxue Li², Kefei Chen¹, and Jianhua Li²

¹ Department of Computer Science and Engineering, Shanghai JiaoTong University
dzheng@sjtu.edu.cn

² School of Information Security Engineering, Shanghai JiaoTong University

³ National Laboratory for Modern Communications, Chengdu

Abstract. Linkable ring signatures can simultaneously provide the properties of anonymity, spontaneity as well as linkability. Linear feedback shift register (LFSR) sequence can be used to shorten the representation of elements in a field. This paper proposes an LFSR-based linkable ring signature scheme, whose main computation operations are performed in *base field* $GF(q)$ whereas security properties are under the state based discrete logarithm assumption (S-DLA) (and a new state based computational assumption weaker than state based decisional Diffie-Hellman assumption). The latter potentially says that the scheme is secure in the *extension field* $GF(q^d)$ (d the stage of the LFSR). All these make our scheme a flexible primitive for ubiquitous computing in which information processing has been thoroughly integrated into everyday objects and activities.

Keywords: Characteristic sequence, Linear feedback shift register, Ring signatures, Anonymity, Linkability.

1 Introduction

For many practical applications or resource-limited environments, it is often desirable to speed up the cryptosystems without notable security degradation. Recently, several cryptosystems have been proposed to shorten the representation of the elements in the finite field [3, 7, 11, 13] by representing them with the coefficients of their minimal polynomials. For instance, Niederreiter [11] designed encryption and key agreement schemes based on general n -th order linear feedback shift register (LFSR) sequences. Giuliani and Gong [3] proposed a general class of LFSR-based key agreement and signature schemes based on n -th order characteristic sequences. Main contributions in these work are that they do not require as much bandwidth as their counterparts based on finite fields.

Ring signature attracts significant attention since its invention [1, 2, 15, 16]. In a ring signature scheme, a user first selects a set U (called a ring) of possible

^{*} Supported by NSFC (No. 60573030, 60673076, 60672068) and NCET (No. NCET-06-0393).

signers including himself, then signs a message using his private key and the public keys of all the members in the ring. The resulting signature can be verified to be generated by some user in the ring, but the identity of the actual signer will not be revealed, hence the signature provides the signer the property of anonymity which cannot be revoked. Linkable ring signatures have a specific property of linkability which means that any one can tell if two ring signatures are generated by using the same private key. In other words, linkability says two signatures by the same actual signer can be identified as such, but the signer remains anonymous. The first linkable ring signature scheme was proposed by Liu *et al.* [10]. The property of linkability is really essential in some scenarios as explained below: (1) Suppose there is an organization that wants to conduct an anonymous and voluntary questionnaires among its members. It is demanded that only legitimate members can submit the questionnaires, and at the same time, each member cannot submit more than one questionnaire. Conventional ring signatures can ensure those who submitted the questionnaires are members of the organization and maintain users' anonymity, but they cannot prevent a member from submitting more than one questionnaire. (2) Another practical instance is to detect double-voting in an e-voting system. Although blind signatures or other cryptographic protocols seem to be able to achieve this goal, yet they require all the users to participate in the *setup* stage even they do not intend to join subsequent protocols.

In current work, we will construct a linkable ring signature scheme based on d -th characteristic sequences generated by an LFSR. Main computation operations of the scheme are performed in the base field $GF(q)$. In fact, besides hash evaluations and addition/multiplications in Z_P , only multiplications of elements in $GF(q)$ are involved in our scheme. This particularly produces a fast system as no exponentiation in $GF(q^d)$ is required. As for its security properties, by resorting to the random oracle methodology, we can show that it is secure under the state based discrete logarithm assumption and state based decisional product Diffie-Hellman assumption as defined in Section 2. Since state based discrete logarithm problem is proved to be equivalent to traditional DLP in $GF(q^d)$ [3], the proposed scheme successfully enhances the security of the system, at the same time, with low computational costs. In other words, to get a system equivalent to one based on extension field $GF(q^d)$, there is no need to compute any exponentiation in $GF(q^d)$.

Organization. The rest of the paper is organized as follows. We first introduce some conceptions and notations related to d -th characteristic sequences in Section 2, then give a security model of linkable ring signatures in Section 3. Section 4 is devoted to the new ring signature scheme based on d -th characteristic sequences. Its formal security arguments are described in Section 5. Finally, concluding remarks are made in Section 6.

Notations. Throughout this paper, let Z_P denote the set $\{0, 1, 2, \dots, P-1\}$, and Z_P^* denote $Z_P \setminus \{0\}$. By $\in_R S$, it means choosing a random element from the set S with a uniform distribution. For an algorithm \mathcal{A} , we use $x \leftarrow \mathcal{A}$ to

denote that \mathcal{A} is executed on some specified input and its output is assigned to the variable x ; if \mathcal{A} is a probabilistic algorithm, we write $x \stackrel{R}{\leftarrow} \mathcal{A}$. Finally, throughout this paper, we often equate a user with his identity, his public key or his secret key without risks of confusion according to the context.

Negligible Function. We say a function $f : \mathbb{N} \rightarrow \mathbb{R}$ is *negligible* if for every constant $c \geq 0$, there exists an integer k_c such that $f(k) < k^{-c}$ for all $k > k_c$.

2 Preliminaries

2.1 LFSR Sequences

We briefly review the necessary about linear feedback shift register. Let q be a prime or a power of prime, $f(x) = x^d + a_1x^{d-1} + a_2x^{d-2} + \dots + a_d$ ($a_i \in GF(q), i = 1, \dots, d$) be an irreducible polynomial over $GF(q)$ with a root α of order P in the extension field $GF(q^d)$. A sequence $s = \{s_j\}$ over $GF(q)$ is said to be an LFSR sequence generated by $f(x)$ if $s_{j+d} = a_1s_{j+d-1} + a_2s_{j+d-2} + \dots + a_ds_j$ ($j \geq 0$).

If an initial state of s is given by $s_j = tr(\alpha^j), j = 0, 1, \dots, d-1$, where $tr(\cdot)$ is the trace map from $GF(q^d)$ to $GF(q)$, then s is called a d -th order characteristic sequence. It is well-known that the period of the d -th characteristic sequence s is equal to the order P of α . Thus we can define $s_j = s_{P+j}$ for all $j \leq 0$, and further consider the sequence $\{s_j\}$ with indices running over all integers. We denote the i -th state of the LFSR sequence as $\bar{s}_i = (s_i, s_{i+1}, \dots, s_{i+d-1})$, and set $A_j = (s_j, s_{2j}, \dots, s_{rj})$, where r is defined by

$$r = \begin{cases} d - 1 & \text{for general } q \text{ and } d, \\ d/2 & \text{if } q = p^2, \text{ and } d \text{ is even,} \\ (d - 1)/2 & \text{if } q = p^2 \text{ and } d \text{ is odd.} \end{cases}$$

Vector A_j can be used to recover the minimal polynomial of $\gamma^j, (\gamma \in GF(q^d), j \in \mathbb{Z})$ [3]. Refer to [4] for more details about the theory of LFSR sequences.

2.2 Complexity Problems

We start this part with several main sequence operations, *i.e.*, SO1, SO2 and SO3, which will be repetitively employed in our scheme. Both SO1 and SO2 can be performed efficiently by the existing algorithms [3], and SO3 can be viewed to be derived from SO1 and SO2 [8]. The following sequence operations can be jointly used to design *smart* and *efficient* cryptographic primitives, including our construction as depicted in Section 3.

- Sequence Operation 1(SO1): *Given A_j and an integer $l(0 < j, l < P)$, to compute A_{jl} .*
- Sequence Operation 2(SO2): *Given states \bar{s}_j and $\bar{s}_l(0 < j, l < P)$, to compute \bar{s}_{j+l} .*
- Sequence Operation 3(SO3): *Given \bar{s}_j and an integer $l(0 < j, l < P)$, to compute \bar{s}_{jl} .*

We proceed to recall the definitions of state based discrete logarithm problem(S-DLP) (and state based decisional Diffie-Hellman problem(S-DDHP)) on which the securities of our scheme are based.

Definition 1. The problem **S-DLP** is, given $(q, n, P, \bar{s}_1, \bar{s}_j)$, to compute j . For a probabilistic polynomial-time (PPT) adversary \mathcal{A} , we define his **advantage** against the S-DLP as

$$Adv_{\mathcal{A}}^{S-DLP} \stackrel{\text{def}}{=} \Pr[\mathcal{A}(\bar{s}_1, \bar{s}_j) = j],$$

where the probability is taken over the random coins consumed by \mathcal{A} .

We say that the (t, ϵ) -**S-DL assumption(S-DLA)** holds, if no t -time adversary \mathcal{A} has advantage at least ϵ in solving the S-DLP.

Definition 2. The problem **S-DDHP** is, given $(q, n, P, \bar{s}_1, \bar{s}_u, \bar{s}_v, \bar{s}_w)$, to decide whether $w = uv$ holds. For a PPT adversary \mathcal{A} , we define his **advantage** against the S-DDHP as

$$Adv_{\mathcal{A}}^{S-DDHP} \stackrel{\text{def}}{=} |\Pr[\mathcal{A}(\bar{s}_1, \bar{s}_u, \bar{s}_v, \bar{s}_{uv}) = 1] - \Pr[\mathcal{A}(\bar{s}_1, \bar{s}_u, \bar{s}_v, \bar{s}_w) = 1]|,$$

where the probability is taken over the random coins consumed by \mathcal{A} .

We say that the (t, ϵ) -**S-DDH assumption** holds, if no t -time adversary \mathcal{A} has advantage at least ϵ in solving the S-DDHP.

It is known that the state based discrete logarithm problem as defined above is computationally equivalent to the traditional DLP in $GF(q^d)$ [14], and that the complexity of breaking S-DDH assumption is equivalent to that of solving decisional Diffie-Hellman problem in the field $GF(q^d)$ [3]. Generally speaking, computational problems such as the DLP are much harder than the DDH, i.e., $DDH \leq DLP$ [6]. Analogical claims come into existence in the state based scenarios [3, 14]. In the following, we further introduce a new problem called *state based decisional product Diffie-Hellman (S-DPDH) problem*. Resorting to the new problem (and S-DLP), we can present our linkable ring signature scheme and construct formal security arguments for the scheme.

Definition 3. The state based decisional product Diffie-Hellman(**S-DPDH**) problem is, given $(q, d, P, \bar{s}_1, \bar{s}_a, \bar{s}_j, \bar{s}_l, \bar{s}_{ac})$, to decide whether $c = jl$ holds. More concretely, for a PPT adversary \mathcal{A} , we define his **advantage** against the problem S-DPDH as

$$Adv_{\mathcal{A}}^{S-DPDH} \stackrel{\text{def}}{=} |\Pr[\mathcal{A}(\bar{s}_1, \bar{s}_a, \bar{s}_j, \bar{s}_l, \bar{s}_{ajl}) = 1] - \Pr[\mathcal{A}(\bar{s}_1, \bar{s}_a, \bar{s}_j, \bar{s}_l, \bar{s}_{ac}) = 1]|,$$

where the probability is taken over the random coins consumed by \mathcal{A} .

S-DPDH assumption says that S-DPDH problem is hard to solve. More precisely, we say that the (t, ϵ) -**S-DPDH assumption(S-DPDHA)** holds, if no t -time adversary \mathcal{A} has advantage at least ϵ in solving the S-DPDH problem.

One can easily note that S-DDHP is just an instance of S-DPDH problem (when we fix $\bar{s}_a = \bar{s}_1$). In other words, S-DPDHA is *no stronger than* S-DDH assumption, which makes the problem S-DPDH independently interesting. It is believed that we prefer to build cryptographic systems on weaker assumptions. In fact, our construction is based on the two weak assumptions S-DLA and S-DPDHA which make the proposed scheme more flexible.

3 Framework of Linkable Ring Signatures

In this section, we will describe the definitions of linkable ring signatures (\mathcal{LRS}) and of the security notions for \mathcal{LRS} .

3.1 Linkable Ring Signatures

We first give an overview for the \mathcal{LRS} model. On the one hand, as original ring signatures, \mathcal{LRS} contains the system initialization algorithm **Setup**, user key generation algorithm **KeyGen**, signature generation algorithm **Sign** and signature verification algorithm **Verify**. On the other hand, \mathcal{LRS} has a special algorithm called **Link** from which any verifier can decide whether two given ring signatures are generated by using the same secret key.

Definition 4. *A linkable ring signature scheme \mathcal{LRS} consists of a tuple of five polynomial-time algorithms:*

Setup: *a probabilistic algorithm, taking as input the security parameter 1^λ , returns a public common parameter $param$. We write $param \stackrel{R}{\leftarrow} \text{Setup}(\lambda)$.*

KeyGen: *a probabilistic key generation algorithm, taking as input the system parameter $param$ and a user's identity $ID \in \{0, 1\}^*$, returns the public/secret key pair (PK, SK) for the user. We write $(PK, SK) \stackrel{R}{\leftarrow} \text{KeyGen}(param, ID)$;*

Sign: *a probabilistic signing algorithm, taking as input the system parameter $param$, a message m , the secret key SK_i of the actual signer with identity ID_i , and the public keys PK_1, \dots, PK_n , returns the resulting signature σ .*

We write $\sigma \stackrel{R}{\leftarrow} \text{Sign}(param, SK_i, PK_1, \dots, PK_n, m)$;

Verify: *a deterministic verification algorithm, taking as input the system parameter $param$, a candidate signature σ on the original message m and the public keys PK_1, \dots, PK_n , returns 1 if (m, σ) is a valid signature, and 0 otherwise.*

We write $(1 \text{ or } 0) \stackrel{R}{\leftarrow} \text{Verify}(param, PK_1, \dots, PK_n, m, \sigma)$;

Link: *The algorithm takes as inputs two valid signatures σ_1 and σ_2 , and returns either 1 for linkable or 0 for unlinkable. We write $(0 \text{ or } 1) \stackrel{R}{\leftarrow} \text{Link}(\sigma_1, \sigma_2)$.*

3.2 Security Notions for Linkable Ring Signatures

Next we will formalize the security notions for \mathcal{LRS} . To this end, we consider the following oracles which together model the abilities of an adversary against \mathcal{LRS} :

- $\mathcal{H}(\cdot)$: a *random oracle* is a theoretical black box that responds to every query with a (truly) random response chosen uniformly from its output domain, except that for any specific query, it responds the same way every time it receives that query. Put another way, a random oracle is a mathematical function mapping every possible query to a random response from its output domain.
- $\mathcal{CO}(\cdot)$: a corruption oracle, upon receiving an identity $ID_i \in \{0, 1\}^*$, returns the corresponding secret key SK_i ;
- $\mathcal{SO}(\cdot, \cdot)$: a signing oracle, taking as input a set of users L and a message m , outputs a signature of L ;

For the security properties of \mathcal{LRS} , there are three aspects we should consider: anonymity, unforgeability and linability.

Let $\Pi = (\text{Setup}, \text{KeyGen}, \text{Sign}, \text{Verify}, \text{Link})$ be an \mathcal{LRS} scheme, n a polynomial and \mathcal{A} an adversary attacking the property of anonymity for DGS. Our model takes insider attack into account by allowing the adversary to corrupt some fraction of the members and thereby come into possession of their secret keys. \mathcal{A} runs in three stages.

In the find stage the adversary is given an initial information string I and the public keys of the members in the ring. It outputs two identities, say, ID_0, ID_1 for uncorrupted members and a message $m \in \{0, 1\}^*$. Based on a challenge bit b , one of the two identities is selected to yield a challenge signature on the message m , which is returned to the adversary, now in its guess stage. Finally \mathcal{A} returns a bit d as its guess of the challenge bit b . In each stage the adversary will output state information that is returned to it in the next stage. We now provide a formal definition.

Definition 5. Let $\Pi = (\text{Setup}, \text{KeyGen}, \text{Sign}, \text{Verify}, \text{Link})$ be an \mathcal{LRS} scheme. For a PPT adversary \mathcal{A} , let n be a polynomial, $b \in \{0, 1\}$, consider the experiment:

Experiment $\text{Exp}_{\Pi, \mathcal{A}}^{\text{IA-b}}(k)$

$I \xleftarrow{R} \text{Setup}(k)$;
 For $i = 0, \dots, n - 1$ do $(x_i, y_i) \xleftarrow{R} \text{KeyGen}(I)$ EndFor;
 $(ID_0, ID_1; m; st) \leftarrow \mathcal{A}^{\mathcal{S}(\cdot, \cdot), \mathcal{CO}(\cdot), \mathcal{H}(\cdot)}(\text{find}, I, y_0, \dots, y_{n-1})$;
 $\sigma \xleftarrow{R} \text{Sign}(I, x_b, y_0, \dots, y_{n-1}, m)$;
 $d \leftarrow \mathcal{A}^{\mathcal{S}(\cdot, \cdot), \mathcal{CO}(\cdot), \mathcal{H}(\cdot)}(\text{guess}, \sigma; st)$;
 return d .

Herein, we naturally require that \mathcal{A} did not submit ID_0, ID_1 to the corruption oracle $\mathcal{CO}(\cdot)$. The advantage of the adversary is defined as

$$\text{Adv}_{\mathcal{A}, \Pi}^{\text{IA}}(k) \stackrel{\text{def}}{=} \Pr[\text{Exp}_{\Pi, \mathcal{A}}^{\text{IA-0}}(k) = 0] - \Pr[\text{Exp}_{\Pi, \mathcal{A}}^{\text{IA-1}}(k) = 0]$$

Let $\Pi = (\text{Setup}, \text{KeyGen}, \text{Sign}, \text{Verify})$ be an \mathcal{LRS} scheme. We say that it is irrevocably anonymous if the function $\text{Adv}_{\mathcal{A}, \Pi}^{\text{IA}}(k)$ is negligible for any poly(k)-time adversary \mathcal{A} and any polynomial n .

Definition 6. Let $\Pi = (\text{Setup}, \text{KeyGen}, \text{Sign}, \text{Verify}, \text{Link})$ be an \mathcal{LRS} scheme. For a PPT adversary \mathcal{A} whose goal is to forge a ring signature, let n be a polynomial, consider the experiment:

Experiment $\text{Exp}_{\Pi, \mathcal{A}}^{\text{UF}}(k)$

$I \xleftarrow{R} \text{Setup}(k);$
 For $i = 0, \dots, n - 1$ do $(x_i, y_i) \xleftarrow{R} \text{KeyGen}(I)$ EndFor;
 $(m^*, \sigma^*) \leftarrow \mathcal{A}^{S(\cdot, \cdot), \mathcal{H}(\cdot)}(I, y_0, \dots, y_{n-1}).$
 \mathcal{A} wins if $\text{Verify}(\text{param}, m^*, \sigma^*, y_0, \dots, y_{n-1}) = 1.$

Above, It is mandated that m^* was not queried to the signing oracle.

The advantage of the adversary is defined as $\text{Adv}_{\mathcal{A}, \Pi}^{\text{UF}}(k) \stackrel{\text{def}}{=} \Pr[\mathcal{A} \text{ wins}].$ Let $\Pi = (\text{Setup}, \text{KeyGen}, \text{Sign}, \text{Verify}, \text{Link})$ be an \mathcal{LRS} scheme. We say that it is unforgeable if the function $\text{Adv}_{\mathcal{A}, \Pi}^{\text{UF}}(k)$ is negligible for any poly(k)-time adversary \mathcal{A} and any polynomial n .

The notion of linkability allows anyone to determine whether two signatures have been issued by the same member in the ring. For simplicity, we say an \mathcal{LRS} scheme is linkable if no member in the group can generate two signatures σ_1, σ_2 such that $\text{Link}(\sigma_1, \sigma_2)$ returns 0. More formally, we have

Definition 7. Let $\Pi = (\text{Setup}, \text{KeyGen}, \text{Sign}, \text{Verify}, \text{Link})$ be an \mathcal{LRS} scheme. For a PPT adversary \mathcal{A} whose goal is to break the property of linkability, let n be a polynomial, consider the experiment:

Experiment $\text{Exp}_{\Pi, \mathcal{A}}^{\text{FL}}(k)$

$I \xleftarrow{R} \text{Setup}(k);$
 For $i = 0, \dots, n - 1$ do $(x_i, y_i) \xleftarrow{R} \text{KeyGen}(I)$ EndFor;
 $\tau \leftarrow \mathcal{A}^{S(\cdot, \cdot), \mathcal{H}(\cdot)}(I, y_0, \dots, y_{n-1})$ where $\tau \in \{0, \dots, n - 1\}.$
 $(m_1, \sigma_1; m_2, \sigma_2) \leftarrow \mathcal{A}^{S(\cdot, \cdot), \mathcal{H}(\cdot)}(I, y_0, \dots, y_{n-1}, x_\tau).$
 return $1 - \text{Link}(\sigma_1, \sigma_2).$

It is mandated that $(m_1, \sigma_1), (m_2, \sigma_2)$ are not output of the signing oracle. The advantage of the adversary is defined as $\text{Adv}_{\mathcal{A}, \Pi}^{\text{FL}}(k) \stackrel{\text{def}}{=} \Pr[\text{Exp}_{\Pi, \mathcal{A}}^{\text{FL}}(k) = 1].$ Let $\Pi = (\text{Setup}, \text{KeyGen}, \text{Sign}, \text{Verify}, \text{Link})$ be an \mathcal{LRS} scheme. We say that it is fully linkable if the function $\text{Adv}_{\mathcal{A}, \Pi}^{\text{FL}}(k)$ is negligible for any poly(k)-time adversary \mathcal{A} and any polynomial n .

4 LFSR-Based Linkable Ring Signatures

Previously, linear feedback shift register(LFSR) is prevalently used to generate pseudo-random sequences which are essential in stream cipher [4]. In [5], Gong

and Harn studied 3-rd order LFSR sequences over a finite field whose cryptographic properties are employed to construct public-key distribution scheme and RSA-type encryption algorithm. Recently, Giulian and Gong [3] proposed an ElGamal-like LFSR-based signature scheme without formal security proof. Provable security is an important research area in cryptography. Cryptographic primitives or protocols without a rigorous proof cannot be regarded as secure in practice. There are many schemes that are originally thought as secure being successfully cryptanalyzed, which clearly indicates the need of formal security assurance. With provable security, we are confident in using cryptographic applications to replace the traditional way in physical world.

Current section is devoted to our LFSR-based linkable ring signature scheme \mathcal{LLRS} . As will be seen from the scheme below, one of its advantages is that its securities rely on hard problems in *extension field* $GF(q^d)$, while all computation operations are performed in *base field* $GF(q)$. This potentially speeds up the run of the scheme without notable security degradation.

More concretely, our scheme \mathcal{LLRS} consists of the following five algorithms where three sequence operations SO1, SO2, SO3 are repeatedly called.

Setup: given a security parameter 1^λ , the algorithm generates the appropriate system parameter as $param = \{q, d, \bar{s}_1, P, H\}$ where H is a cryptographically secure hash function.

KeyGen: a user with identity ID_i randomly chooses his secret key $(w_{i,1}, w_{i,2}) \in Z_P^{*2}$, and generates matching public key $PK_i = (\bar{s}_{w_{i,1}}, \bar{s}_{w_{i,2}})$.

Sign: without loss of generality, we assume that user k is the actual signer. Let $L = \{PK_i, i = 1, \dots, n\}$ be the collection of all the public keys, and m be the message to be signed. Figure.1. illustrates main compositions of algorithm Sign, and each box hits the high spots of each move in the algorithm.

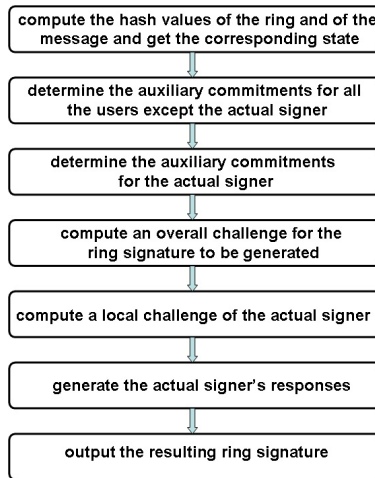


Fig. 1. Ring Signature Generation Algorithm Sign

1. Compute $h = H(L) \bmod P$, $h_1 = H(m) \bmod P$ and obtain \bar{s}_h (\bar{s}_{h_1} , resp.) from \bar{s}_1 and $h(h_1, \text{resp.})$ using SO3. Set $v = hw_{k,1}w_{k,2}$ and get \bar{s}_v . Choose $b \in_R Z_P$, set $t_1 = hw_{i,1}$, $t_2 = h_1b$, $t = t_1 + t_2$, and get \bar{s}_t .
2. For $i = 1, \dots, n(i \neq k)$, perform the following steps.
 - (a) Randomly pick the challenge $0 < c_i < P$, and the responses $0 < z_{i,1}, \dots, z_{i,4} < P$.
 - (b) Denote $d'_{i,1}$ ($d'_{i,2}$, $d'_{i,3}$, $d''_{i,3}$, $d'''_{i,3}$, $d'_{i,4}$, $d''_{i,4}$, $d'''_{i,4}$, resp.) as the product $w_{i,1}c_i$ ($w_{i,2}c_i$, $hz_{i,1}$, $h_1z_{i,3}$, tc_i , $tz_{i,2}$, $h_1(-z_{i,4})$, vc_i , resp.), and set $d_{i,1} = z_{i,1} + d'_{i,1}$, $d_{i,2} = z_{i,2} + d'_{i,2}$, $d_{i,3} = d'_{i,3} + d''_{i,3} + d'''_{i,3}$, $d_{i,4} = d'_{i,4} + d''_{i,4} + d'''_{i,4}$.
 - (c) Compute $\bar{s}_{z_{i,1}}$ ($\bar{s}_{d'_{i,1}}$, $\bar{s}_{d_{i,1}}$, $\bar{s}_{z_{i,2}}$, $\bar{s}_{d'_{i,2}}$, $\bar{s}_{d_{i,2}}$, $\bar{s}_{d'_{i,3}}$, $\bar{s}_{d''_{i,3}}$, $\bar{s}_{d'''_{i,3}}$, $\bar{s}_{d'_{i,4}}$, $\bar{s}_{d''_{i,4}}$, $\bar{s}_{d'''_{i,4}}$, resp.) from the 2-tuple $(\bar{s}_1, z_{i,1})((\bar{s}_{w_{i,1}}, c_i), (\bar{s}_{z_{i,1}}, \bar{s}_{d'_{i,1}}))$, $(\bar{s}_1, z_{i,2})$, $(\bar{s}_{w_{i,2}}, c_i)$, $(\bar{s}_{z_{i,2}}, \bar{s}_{d'_{i,2}})$, $(\bar{s}_h, z_{i,1})$, $(\bar{s}_{h_1}, z_{i,3})$, (\bar{s}_t, c_i) , $(\bar{s}_t, z_{i,2})$, $(\bar{s}_{h_1}, -z_{i,4})$, (\bar{s}_v, c_i) , resp.), and obtain $\bar{s}_{d_{i,3}}$ and $\bar{s}_{d_{i,4}}$ from the 3-tuple $(\bar{s}_{d'_{i,3}}, \bar{s}_{d''_{i,3}}, \bar{s}_{d'''_{i,3}})$ and $(\bar{s}_{d'_{i,4}}, \bar{s}_{d''_{i,4}}, \bar{s}_{d'''_{i,4}})$, respectively.
 - (d) States $\bar{s}_{d_{i,1}}$, $\bar{s}_{d_{i,2}}$, $\bar{s}_{d_{i,3}}$ and $\bar{s}_{d_{i,4}}$ are viewed as the auxiliary commitments for the user i .
3. Randomly pick $r_{k,1}, \dots, r_{k,4}$, let $d_{k,1} = r_{k,1}$, $d_{k,2} = r_{k,2}$, $d'_{k,3} = hr_{k,1}$, $d''_{k,3} = h_1r_{k,3}$, $d_{k,3} = d'_{k,3} + d''_{k,3}$, $d'_{k,4} = tr_{k,2}$, $d''_{k,4} = h_1(-r_{k,4})$, $d_{k,4} = d'_{k,4} + d''_{k,4}$, and compute $\bar{s}_{d_{k,1}}$ ($\bar{s}_{d_{k,2}}$, $\bar{s}_{d'_{k,3}}$, $\bar{s}_{d''_{k,3}}$, $\bar{s}_{d_{k,3}}$, $\bar{s}_{d'_{k,4}}$, $\bar{s}_{d''_{k,4}}$, $\bar{s}_{d_{k,4}}$, resp.) from $(\bar{s}_1, d_{k,1})$ ($(\bar{s}_1, d_{k,2})$, $(\bar{s}_h, r_{k,1})$, $(\bar{s}_{h_1}, r_{k,3})$, $(\bar{s}_{d'_{k,3}}, \bar{s}_{d''_{k,3}})$, $(\bar{s}_t, r_{k,2})$, $(\bar{s}_{h_1}, -r_{k,4})$, $(\bar{s}_{d'_{k,4}}, \bar{s}_{d''_{k,4}})$, respectively). States $\bar{s}_{d_{k,1}}$, $\bar{s}_{d_{k,2}}$, $\bar{s}_{d_{k,3}}$ and $\bar{s}_{d_{k,4}}$ are viewed as the auxiliary commitments for the actual user.
4. Set c_0 as the hash value of m , \bar{s}_v , \bar{s}_t , $\bar{s}_{d_{i,j}}$, for $1 \leq i \leq n, 1 \leq j \leq 4$. Compute $c_k = c_0 - (c_1 + \dots + c_{k-1}) - (c_{k+1} + \dots + c_n)$.
5. Compute the responses of user k :

$$z_{k,1} = r_{k,1} - c_k w_{k,1} \bmod P, \quad z_{k,2} = r_{k,2} - c_k w_{k,2} \bmod P,$$

$$z_{k,3} = r_{k,3} - c_k b \bmod P, \quad z_{k,4} = r_{k,4} - c_k w_{k,2} b \bmod P.$$

6. Output the signature σ as the collection of \bar{s}_v , \bar{s}_t , c_i , $z_{i,j}$, for $1 \leq i \leq n, 1 \leq j \leq 4$.

Remark 1. Although our scheme does not result in signatures with constant size, its particular properties, *i.e.*, low computational costs and high security level, make it adaptable for practical application. And of cause, it is interesting to explore an LFSR-based linkable ring signature scheme with constant size such that it speeds up the system without notable security degradation.

Verify: given a purported signature σ of a ring L on a message m , a verifier can check its validity via the following process.

1. Compute $h = H(L) \bmod P$ and $h_1 = H(m) \bmod P$, then determine \bar{s}_h and \bar{s}_{h_1} from (\bar{s}_1, h) and (\bar{s}_1, h_1) , respectively.
2. For $i = 1, \dots, n$:

- Denote $d'_{i,1}$ ($d'_{i,2}$, $d'_{i,3}$, $d''_{i,3}$, $d''_{i,3}$, $d'_{i,4}$, $d'_{i,4}$, $d'''_{i,4}$, resp.) as the product $w_{i,1}c_i$ ($w_{i,2}c_i$, $hz_{i,1}$, $h_1z_{i,3}$, tc_i , $tz_{i,2}$, $h_1(-z_{i,4})$, vc_i , resp.), and set $d_{i,1} = z_{i,1} + d'_{i,1}$, $d_{i,2} = z_{i,2} + d'_{i,2}$, $d_{i,3} = d'_{i,3} + d''_{i,3} + d'''_{i,3}$, $d_{i,4} = d'_{i,4} + d''_{i,4} + d'''_{i,4}$.
 - Compute $\bar{s}_{z_{i,1}}$ ($\bar{s}_{d'_{i,1}}$, $\bar{s}_{d_{i,1}}$, $\bar{s}_{z_{i,2}}$, $\bar{s}_{d'_{i,2}}$, $\bar{s}_{d_{i,2}}$, $\bar{s}_{d'_{i,3}}$, $\bar{s}_{d''_{i,3}}$, $\bar{s}_{d'''_{i,3}}$, $\bar{s}_{d'_{i,4}}$, $\bar{s}_{d''_{i,4}}$, $\bar{s}_{d'''_{i,4}}$, resp.) from the 2-tuple $(\bar{s}_1, z_{i,1})$ ($(\bar{s}_{w_{i,1}}, c_i)$, $(\bar{s}_{z_{i,1}}, \bar{s}_{d'_{i,1}})$, $(\bar{s}_1, z_{i,2})$, $(\bar{s}_{w_{i,2}}, c_i)$, $(\bar{s}_{z_{i,2}}, \bar{s}_{d'_{i,2}})$, $(\bar{s}_h, z_{i,1})$, $(\bar{s}_{h_1}, z_{i,3})$, (\bar{s}_t, c_i) , $(\bar{s}_t, z_{i,2})$, $(\bar{s}_{h_1}, -z_{i,4})$, (\bar{s}_v, c_i) , resp.).
 - Obtain $\bar{s}_{d_{i,3}}$ and $\bar{s}_{d_{i,4}}$ from the 3-tuple $(\bar{s}_{d'_{i,3}}, \bar{s}_{d''_{i,3}}, \bar{s}_{d'''_{i,3}})$ and $(\bar{s}_{d'_{i,4}}, \bar{s}_{d''_{i,4}}, \bar{s}_{d'''_{i,4}})$, respectively. (Note that $\bar{s}_{d_{i,1}}$ and $\bar{s}_{d_{i,2}}$ are computed in step ii.)
3. Accept the signature if the hash value of m , \bar{s}_v , \bar{s}_t , $\bar{s}_{d_{i,j}}$, matches the sum of c_i , for $1 \leq i \leq n, 1 \leq j \leq 4$.

Link: taking as input two valid signatures $\sigma = (\dots, \bar{s}_v, \dots)$ and $\sigma' = (\dots, \bar{s}_{v'}, \dots)$, the algorithm outputs 1 (for linkable) if $\bar{s}_v = \bar{s}_{v'}$; outputs 0 (for unlinkable), otherwise.

This ends the description of our \mathcal{LLRS} . Consistency requires that $\forall m, m_1, m_2 \in M, j \in \{1, \dots, n\}$, $\text{Verify}(param, PK_1, \dots, PK_n, m, \sigma) = 1$ and $\text{Link}(\sigma_1, \sigma_2) = 1$ hold, where $\sigma = \text{Sign}(param, SK_j, PK_1, \dots, PK_n, m)$, $\sigma_i = \text{Sign}(param, SK_j, PK_1, \dots, PK_n, m_i)$, $i = 1, 2$ and M denotes the message space. One can easily check that the proposed scheme provides the property of consistency. Next we briefly discuss the performance as follows. In fact, above ring signature is an instantiation of the following signature proof-of-knowledge (SPK): $\sigma = SPK\{(w_1, w_2) : \bigvee_{1 \leq i \leq n} (y_{i,1} = \bar{s}_{w_1} \wedge y_{i,2} = \bar{s}_{w_2} \wedge \bar{s}_v = \bar{s}_{hw_1w_2})\}(m)$ which can be viewed as an extension of the following SPK (see [2] and other papers listed in [9] for further details on the notations and theories): $\sigma = SPK\{(x_1, x_2) : \bigvee_{1 \leq i \leq n} (y_{i,1} = g^{x_1} \wedge y_{i,2} = g^{x_2} \wedge v = h^{x_1x_2})\}(m)$.

The online complexity of signature verification requires $4n$ SO2 and $10n + 2$ SO3 operations. All computations are performed by matrix multiplication in the based field $GF(q)$ [3,8], which bring a quite efficient system. The advantages of \mathcal{LLRS} are summarized below:

- i. As will be seen in the coming section, by resorting to the random oracle methodology, its security properties are formally showed under two weak assumptions, i.e., S-DLA and S-DPDHA. This is really interesting since S-DPDHA is weaker than S-DDH assumption.
- ii. Main computation operations are performed in the base field $GF(q)$. In fact, besides hash evaluations and addition/multiplications in Z_P , only multiplications of elements in $GF(q)$ are involved in our scheme. This particularly produces a fast system.

Due to the fact that state based discrete logarithm problem is proved to be equivalent to traditional DLP in extension field $GF(q^d)$ [14] and that the complexity

of breaking S-DDH assumption equates that of solving DDH in $GF(q^d)$ [3], the proposed scheme successfully enhances the security of the system, at the same time, with low computational costs. In other words, to get a system equivalent to one based on extension field $GF(q^d)$, there is no need to compute any exponentiation in $GF(q^d)$.

5 Security Arguments

As for the security properties of our proposed scheme, we have the following results.

Theorem 1. *Suppose \mathcal{A} is a (t, ϵ) -algorithm which forges a linkable ring signature in time at most t with success probability at least ϵ , there exists an algorithm \mathcal{B} which solves the S-DLP.*

Theorem 2. *The proposed scheme provides the property of signer anonymity under the S-DPDHA assumption in the random oracle model.*

Theorem 3. *The proposed scheme provides the property of linkability in the random oracle model under the assumption that S-DLP problem is hard.*

Due to space limitation, we omit the long-winded proofs which are similar to those in [17] according to the special structures of the schemes.

6 Conclusion

Linkable ring signatures can eliminate the registration phase in e-voting systems based on blind signatures and other protocols. From d -th characteristic sequences generated by an LFSR, the paper introduced a linkable ring signature scheme which can be supported by formal security arguments. The scheme enjoys the following attractive features: (i) the proposal provides an option for some applications (*e.g.* e-voting system, E-cash scheme); (ii) an independently interesting assumption (weaker than S-DDH) is introduced; (iii) main computation operations are performed in $GF(q)$; and (iv) security properties of the schemes are equivalent to those of systems based on the multiplication group $GF(q^d)$. The appealing features make our schemes more flexible and highly adaptable to practical applications in the sense that they enhance the security of the system and meanwhile maintain low computational costs as well.

In our scheme, the sizes of public keys and the resulting ring signatures are not ideal as desired. It would be very nice to find an LFSR-based signature scheme in which both the public key and the signature can be represented by short representations. Finally, it would also be nice to develop other applications dependent upon various state based problems.

References

1. Abe, M., Ohkubo, M., Suzuki, K.: 1-out-of-n signatures from a variety of keys. In: *Advances in Cryptology-Asiacrypt 2002*, pp. 415–432 (2002)
2. Camenisch, J., Stadler, M.: Proof systems for general systems of discrete logarithms. ETH Technical Report No, 260 (1997), <ftp://ftp.inf.ethz.ch/pub/publications/tech-reports/>
3. Giuliani, K., Gong, G.: New LFSR-Based cryptosystems and the trace discrete log problem (Trace-DLP). In: *Proceedings of sequences and their applications-SETA 2004*, pp. 298–312 (2004)
4. Golomb, S.: *Shift register sequences*. Laguna Hills, CA: Aegean Park (1982)
5. Gong, G., Harn, L.: Public-key cryptosystems based on cubic finite field extensions. *IEEE Transaction on Information Theory* 24, 2601–2605 (1999)
6. Koblitz, N., Menezes, A.: Another look at generic group. *Cryptology ePrint Archive*, 2006/230, <http://eprint.iacr.org/2006/230>
7. Lenstra, A., Verheul, E.: The XTR public key system. In: *Advances in Cryptology-Crypto 2000*, pp. 1–19 (2000)
8. Li, X., Zheng, D., Chen, K.: LFSR-based signatures with message recovery. *International Journal of Network Security* 4(3), 266–270 (2007)
9. Lipmaa, H.: Proofs of knowledge of certain problems, <http://www.cs.ut.ee/lipmaa/crypto/link/zeroknowledge/pok.php>
10. Liu, J., Wei, V., Wong, D.: Linkable spontaneous anonymous group signature for ad hoc groups. In: *Proceedings of Australasian Conf. Information Security and Privacy-ACISP 2004*, pp. 325–335 (2004)
11. Niederreiter, H.: Finite fields and cryptology. In: *Proceedings of Finite fields, coding theory, and Advances in communications and computing*, Dekker, New York, pp. 359–373 (1992)
12. Rivest, R., Shamir, A., Tauman, Y.: How to leak a secret. In: *Advances in Cryptology-Asiacrypt 2001*, pp. 552–565 (2001)
13. Smith, P., Skinner, C.: A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms. In: *Advances in Cryptology-Asiacrypt 1994*, pp. 357–364 (1994)
14. Tan, C., Yi, X., Siew, C.: On the n-th order shift register based discrete logarithm. *IEICE Transaction on Fundamentals E86-A(5)*, 1213–1216 (2003)
15. Wei, V.: A bilinear spontaneous anonymous threshold signature for ad hoc groups. *Cryptology ePrint Archive*, 2004/039, <http://eprint.iacr.org/>
16. Zhang, F., Kim, K.: ID-Based blind signature and ring signature from pairings. In: *Advances in Cryptology-Asiacrypt 2002*, pp. 535–547 (2002)
17. Zheng, D., Wei, V., Chen, K.: GDH group-based signature scheme with linkability. *Communications, IEE Proceedings* 153(5), 639–644

A Simple and Efficient Key Exchange Scheme Against the Smart Card Loss Problem

Ren-Chiun Wang¹, Wen-Shenq Juang², and Chin-Laung Lei^{1,*}

¹ Department of Electrical Engineering
National Taiwan University
No. 1, Sec. 4, Roosevelt Rd., Taipei, Taiwan 106, R.O.C.
rcwang@fractal.ee.ntu.edu.tw, lei@cc.ee.ntu.edu.tw

² Department of Information Management
Shih Hsin University
No. 1, Lane17, Sec. 1, Mu-Cha Rd., Taipei, Taiwan 116, R.O.C.
wsjuang@cc.shu.edu.tw

Abstract. In a ubiquitous computing environment, a person can use various intelligent devices to obtain his desired services at any time and any place. For convenience, most of these devices are small and of limited power and computation capacity. Therefore, an admired scheme should take these into consideration. In 2006, Lin *et al.* proposed a lightweight authentication scheme only using one-way hash function. However, their scheme is vulnerable to the several security threats. It is the germination of our idea. In this paper, we only require one-way hash function, exclusive OR operation, a smart card, and a memorial password to construct a simple and efficient key exchange scheme to withstand the most known security threats. We also take several merits into our scheme. First, the friendliness and fairness of a user are considered. The user can freely select her/his identity and password for registration and employ the used identity to register repeatedly when the smart card has lost. Second, a user does not need to worry about the damage of the smart card loss problem even if the content of the smart card has been extracted. Our scheme can take care hard security threats and efficient at the same time. Since our scheme does not require any symmetric and asymmetric cryptosystems, the communication and computation cost is very low. Therefore, our scheme is suitable to be applied in ubiquitous computing environments.

Keywords: authentication, hash function, key exchange, password, smart card.

1 Introduction

In a ubiquitous computing environment, each user can use many mobile devices to obtain his service at any time and any place without knowing how to use these devices [18]. These devices could have a low communication and computation capability. When a user wants to get a permitted service from a server,

* Corresponding author.

authentication and key exchange are basic mechanisms due to that the public networks are teem with many uncertainties and security threats are to come out one after the other. In the previous authenticated key exchange schemes, asymmetric cryptosystems such as the Diffie-Hellman [8], ElGamal [11], and RSA [27] schemes are often adopted. However, in those schemes [7,26], the computational complexity and the storage cost are burden.

For mulching the implementation easy and enhancing the performance, many authenticated key exchange schemes were proposed [15,17] by employing symmetric cryptosystems such as DES [10] and AES [1], a memorial password, a one-way hash function [3] and a smart card [21]. However, in those schemes, scholars always discuss to withstand most known security threats over the public networks such as the replay, the impersonation [19,23], the dictionary [2,9], the known-key, and the stolen-verifier [20] attacks, and to enhance the performances of the schemes. Beside the above security threats, in a real life, a user always chooses the same identity and password and employs them to register with different application servers. Unfortunately, this user has to worry about whether the registered information (such as his password) are compromised or not and the security threats of the smart card is stolen by an attacker (also called the smart card loss problem). The administrator of a system could get the password of a registered user and impersonate this user to obtain the service from other servers [29]. The smart card loss problem means that an adversary could employ the information of the smart card to launch some attacks such as the impersonation attack [30,31]. By the way, if a smart card is lost, the holder has to register with the server again using different identities appeared previous schemes. That is not convenient for a user. Therefore, revoking the loss card without changing the user's identity that should be an important issue to take it into consideration.

In 2005, Fan *et al.* [12] proposed a robust authentication scheme based on the concept of symmetric cryptosystem, quadratic residue [13], one-way hash function and exclusive OR operation. In their scheme, a solution was proposed to solve the smart card loss problem. However, the insider attack is still existed, and password changing and key exchange is not supported. Not only that, the storage, the computation and the communication costs of Fan *et al.*'s scheme are still burden. In 2006, Lin *et al.* [24] proposed a lightweight authentication scheme which is constructed by one-way hash function and simple exclusive OR operation without using any symmetric and asymmetric cryptosystems. In their scheme, a solution was proposed to prevent the insider attack. Unfortunately, we show that their scheme is vulnerable to the impersonation, the stolen-verifier, and the smart card lose problem.

From the above description, a secure and efficient smart card-based authenticated key exchange scheme should take the following properties into considerations:

- C_1 : The communication and the computation costs are very low.
- C_2 : Passwords can be chosen and changed freely by the users themselves.
- C_3 : The serious time synchronization problem is not existed in the scheme.

C_4 : The client and the server can confirm the owned session key is correct.

C_5 : The scheme can withstand the smart card loss problem.

C_6 : The user can revoke his loss card without changing the identity.

C_7 : The scheme can withstand the administrator of a system could get the password of a registered user.

C_8 : The scheme can withstand the dictionary attack without the smart card.

C_9 : The scheme can withstand the replay attack.

C_{10} : The scheme can withstand the impersonation attack.

C_{11} : The scheme can withstand the known-key attack.

C_{12} : The scheme can withstand the stolen-verifier attack.

In this paper, we propose a simple and efficient authentication and key exchange scheme without using any symmetric or asymmetric cryptosystems. The proposed scheme provides all of the above properties. The communication and the computation cost is very low in our scheme. Therefore, the proposed scheme is suitable to be applied to ubiquitous computing environments.

The rest of this paper is organized as follows. In the next section, we introduce some definitions and theorems which are used in our scheme. In Section 3, we review Lin *et al.*'s scheme and show that their scheme is insecure. In Section 4, we describe our scheme. In Section 5, we analyze the security of our scheme. In Section 6, we evaluate the performances of our scheme. Finally, we conclude this paper in Section 7.

2 Preliminaries

In this section, we introduce some definitions and theorems of the exclusive OR operation, and one-way hash function in our scheme.

2.1 Exclusive OR Operation

We denote that W is a result of X bit-wise exclusive OR Y . In 2000, Ghanem and Wahab [14] have showed that the exclusive OR operation is secure and the computation is fast. The exclusive OR operation provides the following properties:

1. W , X , and Y are the same bit length.
2. All output results are uniformly distributed in the output domain.
3. We can employ any two of W , X , and Y to retrieve the other one, it is very easy.
4. If the length of W is n bits, there are 2^n different pairs to construct $W = X \oplus Y$.

Theorem 1. Let X and Y are n bits specific values and $W = X \oplus Y$. The probability is negligible to retrieve X and Y when n is large and only given W .

Proof: According to the property 1. of the exclusive OR operation, when X and Y are n bits, we can derive W also is n bits. In the property 4. of the exclusive

OR operation, there are 2^n possible pairs to construct $W = X \oplus Y$. There is a negligible probability which is $\frac{1}{2^n}$ to obtain the specific X and Y from the given W .

2.2 Hash Function

We denote that $h()$ is a one-way hash function. The one-way hash function has the following properties:

1. The function $h()$ can take a message of an arbitrary-length input and produce a message digest of a fixed-length output.
2. The function $h()$ is one-way. Given X , it is easily to calculate $h(X) = Y$. However, given Y , it is hard to derive $h^{-1}(Y) = X$.
3. The function $h()$, given X , it is computationally infeasible to find out X' which is not equal to X to satisfy $h(X') = h(X)$.
4. The function $h()$, it is computationally infeasible to find out any two pairs $X' \neq X$ to satisfy $h(X') = h(X)$.

There are two well-known hash functions SHA-1 [3] and Merkle's hash function [25] which are aimed high-speed software implementations and are current in the public domain. We know many cryptosystems employ hash function for achieving authentication. Now, we also apply it into our scheme.

3 Review of Lin *et al.*'s Scheme

In this section, we review Lin *et al.*'s scheme [23] and show that their scheme is vulnerable to the impersonation, the stolen verifier, and the smart card loss problem attacks.

3.1 Lin *et al.*'s Scheme

Registration phase

- Step 1. A new user U_i selects a password PW_i and a nonce N_i and calculates a verifier $h(PW_i \parallel N_i)$ for registration, where $h()$ is a one-way hash function and \parallel denotes the concatenation of two strings. U_i sends the verifier $h(PW_i \parallel N_i)$ with his identity ID_i to a server through a secure channel.
- Step 2. The server stores the verifier $h(PW_i \parallel N_i)$ into a database and calculates a secret value $K = h(x \parallel ID_i) \oplus h(PW_i \parallel N_i)$, where x is the server's secret key. The server writes the K into a personal smart card and issues it to U_i .

Authentication phase

When U_i wants to get a service from the server, U_i inserts his smart card and keys in his password PW_i . Then the smart card and the server can perform the following steps for authentication.

- Step 1. The smart card first retrieves the stored contents and selects a new nonce N'_i . Then the smart card calculates $C_1 = K \oplus h(PW_i \parallel N_i) = h(x \parallel ID_i)$, $C_2 = h(K) \oplus h(PW_i \parallel N'_i) = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N_i)) \oplus h(PW_i \parallel N'_i)$, and $C_3 = h(C_1 \oplus h(PW_i \parallel N'_i)) = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N'_i))$. Finally, the smart card sends (ID_i, C_2, C_3) to the server.
- Step 2. After receiving the login request, the server retrieves $h(PW_i \parallel N_i)$ from the database, and performs the following steps for verifying the identity of the U_i .
- Step 2.1. Check the format of ID_i . If it is not true, the connection is terminated.
- Step 2.2. Retrieve $h(PW_i \parallel N'_i)$ by computing $h(h(x \parallel ID_i) \oplus h(PW_i \parallel N_i)) \oplus C_2$.
- Step 2.3. Calculate $C'_3 = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N'_i))$ and verify whether C'_3 is equal to C_3 or not. If it holds, the identity of U_i is authenticated; otherwise, the login request is denied. Finally, the server updates the verifier $h(PW_i \parallel N_i)$ with $h(PW_i \parallel N'_i)$.

3.2 Security Analysis of Lin *et al.*'s Scheme

We show that some security threats can work in the Lin *et al.*'s scheme as follows. We use C_x^j to denote the j th login information, where $x = 2$ and 3. The i th login request should include (ID_i, C_2^j, C_3^j) .

The impersonation attack

- Step 1. Assume that, an attacker could tap (j th, $(j + 1)$ th) login information ($C_2^j = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N_i)) \oplus h(PW_i \parallel N'_i)$, $C_3^j = h(h(x \parallel ID_i) \oplus h(PW_i \oplus N'_i))$ and $(C_2^{j+1} = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N'_i)) \oplus h(PW_i \parallel N''_i)$, $C_3^{j+1} = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N''_i))$). Now, we can know the latest verifier is $h(PW_i \parallel N''_i)$ which is used to verify $(j + 2)$ th login request.
- Step 2. The attacker could obtain the latest verifier $h(PW_i \parallel N''_i)$ by computing $C_3^j \oplus C_2^{j+1}$.
- Step 3. Now, the attacker could forge the $(j + 2)$ th login information by calculating $C_2^{j+2} = C_3^{j+1} \oplus h(PW_i \parallel N''_i) = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N''_i)) \oplus h(PW_i \parallel N''_i)$ and $C_3^{j+2} = C_3^{j+1} = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N''_i))$. The attacker sends (C_2^{j+2}, C_3^{j+2}) to the server.
- Step 4. The server will first retrieve $h(PW_i \parallel N''_i)$ from the database and compute $h(h(x \parallel ID_i) \oplus h(PW_i \parallel N''_i)) \oplus C_2^{j+2}$ to get next verifier $h(PW_i \parallel N''_i)$. Then the server verifies whether C_3^{j+2} is equal to $h(h(x \parallel ID_i)) \oplus h(PW_i \parallel N''_i)$ or not. If it holds, the identity of U_i is authenticated; otherwise, the login request is denied. According to the forged (C_2^{j+2}, C_3^{j+2}) , we can know the server will accept this login request, and update the stored verifier $h(PW_i \parallel N''_i)$ with $h(PW_i \parallel N''_i)$.
- Step 5. Using this way, the attacker can iteratively employ C_2^{j+2} and C_3^{j+2} for his later login requests without the smart card and the password of U_i .

The stolen-verifier attack

- Step 1. Assume that, the latest verifier is $h(PW_i \parallel N'_i)$ which is used to verify $(j + 1)$ th login request.
- Step 2. Now, the attacker has stolen the latest verifier $h(PW_i \parallel N'_i)$ and intercepts the last login information (C_2^j, C_3^j) .
- Step 3. Then the attacker can forge the $(j+1)$ th login information (C_2^{j+1}, C_3^{j+1}) , where $C_2^{j+1} = C_3^j \oplus h(PW_i \parallel N'_i) = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N'_i)) \oplus h(PW_i \parallel N'_i)$ and $C_3^{j+1} = C_3^j = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N'_i))$.
- Step 4. This attack is similar to the impersonation attack. As we know, the login request is accepted by the server and the attacker can iteratively employ C_2^{j+1} and C_3^{j+1} for his later login requests without the smart card and the password of U_i .

The smart card loss problem

- Step 1. If the smart card is compromised by an attacker, the attacker can obtain the contents of the smart card, $K = h(x \parallel ID_i) \oplus h(PW_i \parallel N_i)$. The attacker also can intercepts the last and j th login information $(C_2^j = h(K) \oplus h(PW_i \parallel N'_i) = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N_i)) \oplus h(PW_i \parallel N'_i), C_3^j = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N'_i)))$. Now, we know the $(j + 1)$ th verifier is $h(PW_i \parallel N'_i)$.
- Step 2. The attacker can compute $h(K) \oplus C_2^i$ to obtain the $(i + 1)$ th verifier $h(PW_i \parallel N'_i)$.
- Step 3. Then the attacker forges the $(j + 1)$ th login information by calculating $C_2^{j+1} = C_3^j \oplus h(PW_i \parallel N'_i) = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N'_i)) \oplus h(PW_i \parallel N'_i)$ and $C_3^{j+1} = C_3^j = h(h(x \parallel ID_i) \oplus h(PW_i \parallel N'_i))$.
- Step 4. As we know, the forged login request will be accepted by the server and the attacker can iteratively employ C_2^{i+1} and C_3^{i+1} for his later login requests without the password of U_i .

4 Our Proposed Scheme

The intention of our scheme is to propose a simple and efficient key exchange scheme against the potential and serious threats that are the insider attack and the smart card loss problem. We divide the scheme into two phases: the registration phase and the authentication phase. We start to introduce the proposed scheme as follows.

Registration phase

- Step 1. A new user U_i selects a password PW_i and a random number N_i and calculates a verifier $h(PW_i \parallel N_i)$ for registration, where $h()$ is a one-way hash function and \parallel denotes the concatenation of two strings. U_i sends the verifier $h(PW_i \parallel N_i)$ with his identity ID_i to a server through a secure channel.

- Step 2. The server calculates a secret value $K = h(x \parallel ID_i \parallel CID_i)$, where x is the server's secret key and CID_i is the smart card's identifier. The server writes (ID_i, K) into a personal smart card and issues it to the U_i . The server stores $(ID_i, CID_i, h(PW_i \parallel N_i))$ into a database.
- Step 3. U_i writes N_i into the smart card. Finally, the contents of the smart card is (ID_i, K, N_i) .

Authentication phase

When U_i wants to establish a secure conversation with the server, U_i inserts his smart card and keys in the password PW_i . Then the smart card and the server can perform the following steps for agreeing a common session key.

Smart cards

- Step 1. Retrieve the contents (ID_i, K, N_i) and select a random number N'_i .
- Step 2. Calculate $C_1 = h^2(PW_i \parallel N_i)$, $C_2 = C_1 \oplus h^2(PW_i \parallel N'_i)$, $K_1 = h(h(PW_i \parallel N_i) \parallel K)$, and $C_3 = h(K_1 \parallel h^2(PW_i \parallel N'_i))$.
- Step 3. Send (ID_i, C_2, C_3) to the server.

Server

- Step 4. Check whether the ID_i is existed in the database or not. If not, the connection is terminated; otherwise, retrieve $(ID_i, CID_i, h(PW_i \parallel N_i))$ from the database.
- Step 5. Calculate $V_1, h(x \parallel ID_i \parallel CID_i), K'_1$, and C'_3 , where $V_1 = h^2(PW_i \parallel N_i) \oplus C_2 = h^2(PW_i \parallel N'_i)$, $K'_1 = h(h(PW_i \parallel N_i) \parallel h(x \parallel ID_i \parallel CID_i))$ and $C'_3 = h(K'_1 \parallel V_1)$.
- Step 6. Verify whether C_3 is the same as the C'_3 or not. If not, the connection is terminated.
- Step 7. Select a random number N_s and calculate (C_4, SK, S_1) , where $C_4 = N_s \oplus V_1$, $SK = h(K'_1 \parallel N_s \parallel V_1)$, and $S_1 = h(K'_1 \parallel SK)$.
- Step 8. Send (C_4, S_1) to U_i .

Smart cards

- Step 9. Retrieve N'_s by computing $h^2(PW_i \parallel N'_i) \oplus C_4$.
- Step 10. Calculate $SK = h(K_1 \parallel N'_s \parallel h^2(PW_i \parallel N'_i))$, and $T_1 = h(K_1 \parallel SK)$.
- Step 11. Verify whether S_1 is the same as the T_1 or not. If not, the connection is terminated.
- Step 12. Calculate $C_5 = h(K_1) \oplus h(PW_i \parallel N'_i)$ and send C_5 back to the server.
- Step 13. Update N_i with N'_i .

Server

- Step 14. Calculate $V_2 = C_5 \oplus h(K'_1) = h(PW_i \parallel N'_i)$.
- Step 15. Verify whether $h(V_2)$ is equal to V_1 or not. If not, the connection is terminated; otherwise, accept the session key SK and update $h(PW_i \parallel N_i)$ with V_2 .

Password changing phase

When U_i wants to renew his password, U_i does not need to extra perform a password changing phase. U_i can first choose a new password $PW_{i_{new}}$ and a new random number N'_i . Then U_i can perform the steps of the authentication phase to achieve the purpose of changing password. Finally, the server will store a new verifier $h(PW_{i_{new}} \parallel N'_i)$.

5 Security Analysis

We use the logic analysis method [4,?] to prove the authentication of the proposed scheme which is described in appendix A and the heuristic security analysis to show that our scheme can withstand most of the known security threats. Before we analyze the proposed scheme, we first assume that an adversary has an ability to collect all message flows between a client and a server. For instance, when the last message flow is intercepted, the adversary can obtain $(C_2 = h^2(PW_i \parallel N_i) \oplus h^2(PW_i \parallel N'_i), C_3 = h(K_1 \parallel h^2(PW_i \parallel N'_i)), C_4 = N_s \oplus h^2(PW_i \parallel N'_i), S_1 = h(K'_1 \parallel SK), C_5 = h(K_1) \oplus h(PW_i \parallel N'_i))$, where $K = h(x \parallel ID_i \parallel CID_i)$, $K_1 = h(h(PW_i \parallel N_i) \parallel K)$, $SK = h(K_1 \parallel N'_s \parallel h^2(PW_i \parallel N'_i))$, and $K_1 = K'_1$.

5.1 Revoking the Loss Card Without Changing the User’s Identity

When a user registers from a server, the server will issue a personal smart card to him, where the content of the smart card is $(ID_i, K = h(x \parallel ID_i \parallel CID_i), N_i)$, the CID_i is the smart card’s identifier and the server stores $(ID_i, CID_i, h(PW_i \parallel N_i))$ in his database.

When the smart card has lost, the user can use the same identity ID_i to register again, the content of the new smart card becomes $(ID_i, K = h(x \parallel ID_i \parallel CID'_i), N_{i_{new}})$, where the CID'_i is a new identifier of the smart card and the server’s verifier are to become $(ID_i, CID'_i, h(PW_i \parallel N_{i_{new}}))$. Only the new card can achieve in the scheme.

This property provides us a protection: even if the adversary has older loss card or user’s password, the server can employ CID'_i to discriminate them.

5.2 The Dictionary Attack

On-line dictionary attack: This is an unavoidable attack and it requires the server joins this attack. The server can detect the failed times and take appropriate login times to prevent this attack, where the failed times means if the authentication phase is not finished, the failed times plus one. All password-based schemes can withstand this attack.

Off-line dictionary attack: If the adversary intercepts the communicated messages, the adversary can directly make a dictionary attack at off-line. However, this attack will be failed due to the adversary has no $(N_i, N'_i, h(x \parallel ID_i \parallel CID_i))$.

5.3 The Smart Card Loss Problem

After j th login request is accepted by the server, if the smart card of a holder is stolen by an adversary, the adversary still can not launch some attacks on our scheme. Note that, the adversary can obtain the smart card's contents that are $(ID_i, K = h(x \parallel ID_i \parallel CID_i), N'_i)$ and the $(j + 1)$ th verifier is $h(PW_i \parallel N'_i)$ which is stored in the server. We analyze some possible situations as follows.

Situation 1: The adversary directly makes the dictionary attack on the intercepted information $(C_2, C_3, C_4, S_1, C_5)$ with the smart card. We can find this attack is not succeed due to the adversary does not have the random number N_i .

Situation 2: The adversary's target is to get one of $h(PW_i \parallel N_i)$, PW_i and N_i and employs it to verify the guessed password from the intercepted messages with the smart card. However, we observe the adversary can not derive some valuable information due to the properties of the one-way hash function.

Situation 3: If the adversary wants to forge a login request, the adversary may have to guess a password PW'_i and to select a random number $N_{i_{attacker}}$. Then the adversary computes $(C_{2_{attacker}} = h^2(PW'_i \parallel N_{i_{attacker}}) \oplus h^2(PW'_i \parallel N'_i), C_{3_{attacker}} = h(K_{1_{attacker}} \parallel h^2(PW'_i \parallel N_{i_{attacker}})))$ and sends $(ID_i, C_{2_{attacker}}, C_{3_{attacker}})$ to the server, where $K_{1_{attacker}} = h(h(PW'_i \parallel N_{i_{attacker}}) \parallel K)$.

Before the server sends a response (C_4, S_1) back, the server first verifies whether C_3 is equal to C'_3 or not. Now, if the adversary receives (C_4, S_1) , it denotes the adversary guesses the password correctly. Obviously, this is a on-line password guessing attack. The server can detect the failed times and permit appropriate login times to prevent this attack.

5.4 The Insider Attack

When a valid client submits his identity ID_i and a verifier $h(PW_i \parallel N_i)$ to the server, the server's administrator can not get PW_i or launch a off-line dictionary attack on $h(PW_i \parallel N_i)$ without the random number N_i . Therefore, the insider attack can not work in our scheme.

5.5 The Replay Attack

After j th login request is accepted by the server, we know the $(j + 1)$ th verifier becomes $h(PW_i \parallel N'_i)$. Now, if the adversary replays (ID_i, C_2, C_3) to the server, the server will calculate $h^2(PW_i \parallel N'_i) \oplus C_2$ to get $h^2(PW_i \parallel N_i)$ and verify whether $C'_3 = h(K_1 \parallel h^2(PW_i \parallel N_i))$ is the same as C_3 . Then we can find C_3 is not equal to C'_3 . The adversary can not replay a used login request to impersonate this client.

5.6 The Impersonation Attack

In our scheme, even if the adversary gets all message flows from the communicated channel with the smart card, the adversary still can not launch a off-line

dictionary attack or derive some valuable information due to the properties of one-way hash function and the detail is described in 5.3.

5.7 The Known-Key Attack

Once a used session key $SK = h(K_1 \parallel N'_s \parallel h^2(PW_i \parallel N'_i))$ is compromised, the adversary still can not get any advantage. The adversary could employ the session key to launch the following attacks:

Situation 1: Make a off-line dictionary attack on the session key directly. The adversary can not succeed without the knowledge of (K_1, N_s, N'_i) .

Situation 2: Retrieve some valuable information from the intercepted messages. The adversary can not succeed due to the properties of the one-way hash function.

5.8 The Stolen-Verifier Attack

When the latest verifier $h(PW_i \parallel N'_i)$ has stolen by an adversary, the adversary can perform the following situations to launch some attacks.

Situation 1: Make a off-line dictionary attack on the verifier. The adversary can not succeed without N'_i .

Situation 2: Retrieve some valuable information from the intercepted messages by using the verifier. The adversary can get $(h^2(PW_i \parallel N_i), N_s, h(K_1))$ from C_2 , C_4 and C_5 respectively. However, the adversary still can not launch the off-line dictionary attack from these information without N_i , derive the previous session keys and forge next login request without K_1 .

6 Performance Considerations

In this section, we compare the computational complexity and satisfaction of the properties with the previous schemes for evaluating our scheme. We assume that: the output length of a one-way hash function is 160 bits; the output length of a symmetric cryptosystem is 128 bits; and the output length of an asymmetric cryptosystem is 1024 bits.

6.1 Efficiency Comparison

To analyze the computational complexity, we define some notations: T_h denotes the time of one hashing function operation, T_{exp} denotes the time of one modular exponential operation, T_{sym} denotes the time of one symmetric encryption or decryption, T_{sqr} denotes the time for one modular square root, T_{\oplus} denotes the time of one XOR operation, The length of an identity is 32-bit, the length of a random number is 64-bit, and the length of a timestamp is 32-bit. Then we use table [11](#) to show that our comparison.

Table 1. Comparisons of computation and communication costs between our scheme and the related schemes

| | Registration phase | Authentication phase | The size of the transferred messages |
|-----------------------------------|----------------------|--|--|
| Our scheme | $2T_h$ | $17T_h + 6T_{\oplus}$ | $ID + 5 \times 160$ = 832 bits |
| Liaw <i>et al.</i> 's scheme [22] | $1T_h + 1T_{\oplus}$ | $3T_h + 2T_{\oplus} + 2T_{exp} + 4T_{symm}$ | $ID + 1 \times 160 + R + 128$ = 384 bits |
| Juang's scheme [16] | $1T_h + 1T_{\oplus}$ | $5T_h + 1T_{\oplus} + 6T_{symm}$ | $ID + R + 3 \times 128$ = 480 bits |
| Chen-Yeh's scheme [6] | $1T_h + 2T_{\oplus}$ | $13T_h + 6T_{\oplus}$ | $ID + 4 \times 160$ = 672 bits |
| Fan <i>et al.</i> 's scheme [12] | $2T_h + 1T_{symm}$ | $5T_h + 2T_{\oplus} + 1T_{sqr} + 1T_{mul} + 1T_{symm}$ | $ID + 3 \times 160 + 1 \times 1024$ = 1536 bits |
| Shieh-Wang's scheme [28] | $1T_h + 2T_{\oplus}$ | $9T_h + 4T_{\oplus}$ | $ID + 3 \times 160 + 4 \times T$ = 640 bits |
| Lin <i>et al.</i> 's* scheme [24] | $2T_h + 1T_{\oplus}$ | $7T_h + 6T_{\oplus}$ | $ID + 2 \times 160$ = 352 bits |

* The scheme is only to provide an unilateral authentication.

Table 2. Comparisons of satisfaction of the properties between our scheme and the related schemes

| | C_1 | C_2 | C_3 | C_4 | C_5 | C_6 | C_7 | C_8 | C_9 | C_{10} | C_{11} | C_{12} |
|-----------------------------------|---------------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|
| Our scheme | Extremely Low | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Liaw <i>et al.</i> 's scheme [22] | High | Yes | Yes | Yes | No | No | No | Yes | Yes | Yes | Yes | Yes |
| Juang's scheme [16] | Low | No | Yes | Yes | No | No | No | Yes | Yes | Yes | Yes | Yes |
| Chen-Yeh's scheme [6] | Extremely low | No | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes |
| Fan <i>et al.</i> 's scheme [12] | High | No | Yes | No | Yes | Yes | No | Yes | Yes | Yes | * | Yes |
| Shieh-Wang's scheme [28] | Extremely low | No | No | No | No | No | No | Yes | Yes | Yes | Yes | Yes |
| Lin <i>et al.</i> 's scheme [24] | Extremely low | No | Yes | No | No | No | No | Yes | Yes | No | * | No |

* Denotes the scheme does not support a key exchange phase.

6.2 Functionality Comparison

A secure and efficient key exchange scheme should provide some properties which is described in the Section 1. Now, we compare satisfaction of the properties with the previous scholarship and use table 2 to show that our comparisons.

From the Subsections 6.1 and 6.2, our scheme requires fewer computation cost to satisfy all of the properties. To do that, our scheme does not require any symmetric and asymmetric cryptosystems to protect the communicated messages. Therefore, our scheme is easy to be applied in ubiquitous computing environments.

7 Conclusions

In this paper, we have shown that Lin *et al.*'s scheme is insecure. We also have proposed a simple and efficient key exchange scheme to withstand the administrator of a system could get the password of a registered user and the smart card loss problem without using any symmetric and asymmetric cryptosystems. We also take the friendliness and fairness of the users into our consideration. Our scheme's the computation cost and the communicated message flows are low. Therefore, our scheme is suitable to be applied in many ubiquitous computing environments.

Acknowledgement. This work is supported in part by the National Science Council under the Grant NSC 96-2628-E-002-182-MY3, NSC 95-2221-E-128-004-MY2, and by the Taiwan Information Security Center (TWISC), National Science Council under the Grants No. NSC 96-2219-E-001-001.

References

1. Advanced Encryption Standard, <http://csrc.nist.gov/encryption/aes/>
2. Bellare, M., Pointcheval, D., Rogaway, P.: Authenticated and key exchange secure against dictionary attacks. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 139–155. Springer, Heidelberg (2000)
3. Biham, E., Chen, R., Joux, A., Carribault, P., Jalby, W., Lemuet, C.: Collisions in SHA-0 and reduced SHA-1. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 36–57. Springer, Heidelberg (2005)
4. Burrows, M., Abadi, M., Needham, R.: A logic of authentication. ACM Transactions on Computer Systems (TOCS) 8(1), 18–36 (1990)
5. Buttyán, L., Staamann, S., Wilhelm, U.: A simple logic for authentication protocol design. In: Proc. of 11th IEEE Computer Security Foundations Workshop, Rockport, Massachusetts, USA, June 9–11, pp. 153–162 (1998)
6. Chen, Y.-C., Yeh, L.-Y.: An efficient nonce-based authentication with key agreement. Applied Mathematics and Computation 169(2), 982–994 (2005)
7. Chien, H.-Y., Wang, R.-C., Yang, C.-C.: Note on robust and simple authentication protocol. The Computer Journal 48(1), 27–29 (2005)
8. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. on Information Theory IT-22, 644–654 (1976)
9. Ding, Y., Horster, P.: Undetected on-line password guessing attacks. ACM Operating Systems Review 29(4), 77–86 (1995)
10. Eberle, H.: A high-speed DES implement for network applications. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 527–545. Springer, Heidelberg (1993)

11. ElGamal, T.: A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. on Information Theory* IT-31, 469–472 (1985)
12. Fan, C.-I., Chan, Y.-C., Zhang, Z.-K.: Robust remote authentication scheme with smart cards. *Computers & Security* 24, 619–628 (2005)
13. Fan, C.-I., Lei, C.-L.: Efficient blind signature schemes based on quadratic residues. *IEE Electronics Letters* 32(9), 811–813 (1996)
14. Ghanem, S.M., Wahah, H.A.: A simple XOR-based technique for distributing group key secure multicasting. In: *Proc. of 5th IEEE Symposium on Computers and Communications*, pp. 166–171 (2000)
15. Juang, W.-S.: Efficient multi-server password authenticated key agreement using smart cards. *IEEE Trans. on Consumer Electronics* 50(1), 251–255 (2004)
16. Juang, W.-S.: Efficient password authenticated key agreement using smart cards. *Computers & Security* 23, 167–173 (2004)
17. Juang, W.-S.: Efficient three-party key exchange using smart cards. *IEEE Trans. on Consumer Electronics* 50(2), 619–624 (2004)
18. Juang, W.-S.: Efficient User Authentication and Key Agreement in Ubiquitous Computing. In: Gavrilova, M., Gervasi, O., Kumar, V., Tan, C.J.K., Taniar, D., Laganà, A., Mun, Y., Choo, H. (eds.) *ICCSA 2006. LNCS*, vol. 3983, pp. 396–405. Springer, Heidelberg (2006)
19. Ku, W.-C., Chang, S.-T.: Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards. *IEICE Trans. on communications* E88-B(5), 2165–2167 (2005)
20. Ku, W.-C., Tsai, H.-C., Tsaur, M.-J.: Stolen-verifier attack on an efficient smart card-based one-time password authentication scheme. *IEICE Trans. on communications* E87-B(8), 2374–2376 (2004)
21. Lamport, L.: Password authentication with insecure communication. *Communications of the ACM* 24, 770–772 (1981)
22. Liaw, H.-T., Lin, J.-F., Wu, W.-C.: An efficient and complete remote user authentication scheme using smart cards. *Mathematical and Computer Modelling* 44, 223–228 (2006)
23. Lin, C.-L., Hung, C.-P.: Impersonation attack on two-gene-relation password authentication protocol 2GR. *IEICE Trans. on communications* E89-B(12), 3425–3427 (2006)
24. Lin, C.-W., Tsai, C.-S., Hwang, M.-S.: A new strong-password authentication scheme using one-way hash functions. *International Journal of Computer and Systems Sciences* 45(4), 623–626 (2006)
25. Merkle, R.C.: One-way hash functions and DES. In: Brassard, G. (ed.) *CRYPTO 1989. LNCS*, vol. 435, pp. 428–446. Springer, Heidelberg (1990)
26. Peyravian, M., Jeffries, C.: Secure remote user access over insecure networks. *Computers Communications* 29, 660–667 (2006)
27. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signature and public key cryptosystems. *Communications of the ACM* 21, 120–126 (1978)
28. Shieh, W.-G., Wang, J.-M.: Efficient remote mutual authentication and key agreement. *Computers & Security* 25, 72–77 (2006)
29. Ku, W.-C., Chen, C.-M., Lee, H.-L.: Cryptanalysis of a variant of Peyravian-Zunic's password authentication scheme. *IEICE Trans. on Communications* E86-B, 1682–1684 (2003)
30. Ku, W.-C., Chen, S.-M.: Weakness and improvement of an efficient password based remote user authentication scheme using smart cards. *IEEE Trans. on Consumer Electronics* 50(1), 204–207 (2004)

31. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart card security under the threat of power analysis attacks. *IEEE Trans. on Computers* 51(5), 541–552 (2002)

Appendix A

We use the logic analysis method [45] to prove the authentication of the proposed scheme.

Notations

- P, Q : two principals.
- C : channel.
- C_c : a channel C which can be read only if c is known.
- X : message, which could be data or formula or both.
- $C(X)$ or $C_C(X)$: message X on channels C or C_C .
- $r(C)$ and $w(C)$: the set of readers and writers of channel C .
- $P \in r(C)$: a principal P is one of readers of channel C .
- $P \in w(C)$: a principal P is one of writers of channel C .
- ϕ : formula.
- $P \triangleleft C(X)$: P sees $C(X)$.
- $P \triangleleft X|C$: P sees X through C .
- $P \triangleleft X$: P sees X .
- $\#(X)$: X is fresh.
- $P \sim X$: P once said X .
- $P \|\sim X$: P has recently said X .
- $P \equiv \phi$: P believes ϕ .
- $\phi_1 \longrightarrow \phi_2$: ϕ_1 implies ϕ_2 .

We describe the synthetic rules which are used to prove the proposed scheme as follows:

- (Syn. 1): In order to achieve a goal G , all new goals G_1, G_2, \dots have to be achieved.

$$\begin{array}{l}
 G \\
 \hookrightarrow G_1 \\
 \hookrightarrow G_2 \\
 \hookrightarrow \dots
 \end{array}$$
- (Syn. 2): If a principal P wants to see a message X arrived through a channel C , P has to see $C(X)$ and can read C .

$$\begin{array}{l}
 P \equiv (P \triangleleft X|C) \\
 \hookrightarrow P \triangleleft C(X) \\
 \hookrightarrow P \in r(C)
 \end{array}$$
- (Syn. 3): If a principal P wants to believe a formula ϕ , the P has to believe a formula ϕ' and the implication $\phi' \longrightarrow \phi$.

$$\begin{array}{l}
 P \equiv \phi \\
 \hookrightarrow P \equiv \phi' \\
 \hookrightarrow P \equiv (\phi' \longrightarrow \phi)
 \end{array}$$

Proof of the authentication phase: When a user U_i wants to access the resource from a remote server S , the transmitted messages between them are as follows:

- (i) $U_i \longrightarrow S: ID_i, C_1 \oplus h^2(PW_i \parallel N'_i), C_3$
- (ii) $S \longrightarrow U_i: N_s \oplus V_1, h(K'_1 \parallel SK)$
- (iii) $U_i \longrightarrow S: h(K_1) \oplus h(PW_i \parallel N'_i)$

We transfer the messages to the description in the following.

- (i) $S \triangleleft C_{C_1} (h^2(PW_i \parallel N'_i))$
- (ii) $U_i \triangleleft C_{V_1} (N_s), C_{K'_1} (SK)$
- (iii) $S \triangleleft C_{K_1} (h(PW_i \parallel N'_i))$

We also identify the following assumptions.

- (A1) $U_i \in r(C_{C_1})$: U_i can read channel C_{C_1} .
- (A2) $S \in r(C_{C_1})$: S can read channel C_{C_1} .
- (A3) $U_i \models (w(C_{C_1})) = (U_i, S)$: U_i believes that only S and U_i can write channel C_{C_1} .
- (A4) $S \models (w(C_{C_1})) = (U_i, S)$: S believes that only U_i and S can write channel C_{C_1} .
- (A5) $U_i \in r(C_{V_1})$: U_i can read channel C_{V_1} .
- (A6) $S \in r(C_{V_1})$: S can read channel C_{V_1} .
- (A7) $U_i \models (w(C_{V_1})) = (U_i, S)$: U_i believes that only S and U_i can write channel C_{V_1} .
- (A8) $S \models (w(C_{V_1})) = (U_i, S)$: S believes that only U_i and S can write channel C_{V_1} .
- (A9) $U_i \in r(C_{K'_1})$: U_i can read channel $C_{K'_1}$.
- (A10) $S \in r(C_{K'_1})$: S can read channel $C_{K'_1}$.
- (A11) $U_i \models (w(C_{K'_1})) = (U_i, S)$: U_i believes that only S and U_i can write channel $C_{K'_1}$.
- (A12) $S \models (w(C_{K'_1})) = (U_i, S)$: S believes that only U_i and S can write channel $C_{K'_1}$.
- (A13) $U_i \models ((U_i \triangleleft N_s \mid C_{V_1}) \longrightarrow U_i \xleftrightarrow{SK} S)$: U_i believes that he sees N_s through channel C_{V_1} implies that U_i and S share SK .
- (A14) $S \models ((S \triangleleft h^2(PW_i \parallel N'_i) \mid C_{C_1}) \longrightarrow U_i \xleftrightarrow{SK} S)$: S believes that he sees $h^2(PW_i \parallel N'_i)$ through channel C_{C_1} implies that U_i and S share SK .
- (A15) $U_i \models ((U_i \triangleleft SK \mid C_{K'_1}) \longrightarrow (S \models U_i \xleftrightarrow{SK} S))$: U_i believes that he sees SK through channel $C_{K'_1}$ implies that S believes that U_i and S share SK .
- (A16) $S \models ((S \triangleleft h(PW_i \parallel N'_i) \mid C_{K_1}) \longrightarrow (U_i \models U_i \xleftrightarrow{SK} S))$: S believes that he sees $h(PW_i \parallel N'_i)$ through channel C_{K_1} implies that U_i believes that U_i and S share SK .

There are four goals need to be achieved in our scheme for proving the authentication property.

- (Goal 1:) $U_i \equiv U_i \xleftrightarrow{SK} S$;
- (Goal 2:) $S \equiv U_i \xleftrightarrow{SK} S$;
- (Goal 3:) $U_i \equiv (S \equiv U_i \xleftrightarrow{SK} S)$
- (Goal 4:) $S \equiv (U_i \equiv U_i \xleftrightarrow{SK} S)$

We use the above synthetic rules and assumptions to prove our goals.

1. Prove Goal 1: $U_i \equiv U_i \xleftrightarrow{SK} S$

Proof. By using (Syn. 3), we know that:

$$U_i \equiv U_i \xleftrightarrow{SK} S$$

$$\hookrightarrow U_i \equiv (U_i \triangleleft N_s \mid C_{V_1}) \tag{1}$$

$$\hookrightarrow U_i \equiv ((U_i \triangleleft N_s \mid C_{V_1}) \longrightarrow U_i \xleftrightarrow{SK} S) \tag{2}$$

We use the assumption (A13) to achieve the new goal (2). Then we employ (Syn. 2) to show that our new goal (1).

$$U_i \equiv (U_i \triangleleft N_s \mid C_{V_1})$$

$$\hookrightarrow U_i \triangleleft C_{V_1}(N_s) \tag{3}$$

$$\hookrightarrow U_i \in r(C_{V_1}) \tag{4}$$

The new goals (3) and (4) are existed and achieved in the message 2 of the scheme and the assumption (A5).

From the above, the Goal 1: $U_i \equiv U_i \xleftrightarrow{SK} S$ is proved. □

2. Prove Goal 2: $S \equiv U_i \xleftrightarrow{SK} S$

Proof. By using (Syn. 3), we know that:

$$S \equiv U_i \xleftrightarrow{SK} S$$

$$\hookrightarrow S \equiv (S \triangleleft h^2(PW_i \parallel N'_i) \mid C_{C_1}) \tag{5}$$

$$\hookrightarrow S \equiv ((S \triangleleft h^2(PW_i \parallel N'_i) \mid C_{C_1}) \longrightarrow U_i \xleftrightarrow{SK} S) \tag{6}$$

We use the assumption (A14) to achieve the new goal (6). Then we employ (Syn. 2) to show that our new goal (5).

$$S \equiv (S \triangleleft h^2(PW_i \parallel N'_i) \mid C_{C_1})$$

$$\hookrightarrow S \triangleleft C_{C_1}(h^2(PW_i \parallel N'_i)) \tag{7}$$

$$\hookrightarrow S \in r(C_{C_1}) \tag{8}$$

The new goals (7) and (8) are existed and achieved in the message 1 of the scheme and the assumption (A2).

From the above, the Goal 2: $S \equiv U_i \xleftrightarrow{SK} S$ is proved. □

3. Prove goal 3: $U_i \models (S \models U_i \xleftrightarrow{SK} S)$

Proof. By using (Syn. 3), we know that:

$$U_i \models (S \models U_i \xleftrightarrow{SK} S)$$

$$\hookrightarrow U_i \models (U_i \triangleleft SK \mid C_{K'_1}) \quad (9)$$

$$\hookrightarrow U_i \models ((U_i \triangleleft SK \mid C_{K'_1})$$

$$\hookrightarrow S \models U_i \xleftrightarrow{SK} S) \quad (10)$$

We use the assumption (A15) to achieve the new goal (10). Then we employ (Syn. 2) to show that our new goal (9).

$$U_i \models (U_i \triangleleft SK \mid C_{K'_1})$$

$$\hookrightarrow U_i \triangleleft C_{K'_1}(SK) \quad (11)$$

$$\hookrightarrow U_i \in r(C_{K'_1}) \quad (12)$$

The new goals (11) and (12) are existed and achieved in the message 2 of the scheme and the assumption (A9).

From the above, the Goal 3: $U_i \models (S \models U_i \xleftrightarrow{SK} S)$ is proved. \square

4. Prove goal 4: $S \models (U_i \models U_i \xleftrightarrow{SK} S)$

Proof. By using (Syn. 3), we know that:

$$S \models (U_i \models U_i \xleftrightarrow{SK} S)$$

$$\hookrightarrow S \models (S \triangleleft h(PW_i \parallel N'_i) \mid C_{K_1}) \quad (13)$$

$$\hookrightarrow S \models (S \triangleleft h(PW_i \parallel N'_i) \mid C_{K_1})$$

$$\hookrightarrow U_i \models U_i \xleftrightarrow{SK} S) \quad (14)$$

We use the assumption (A16) to achieve the new goal (14). Then we employ (Syn. 2) to show that our new goal (13).

$$S \models (S \triangleleft h(PW_i \parallel N'_i) \mid C_{K_1})$$

$$\hookrightarrow S \triangleleft C_{K_1}(h(PW_i \parallel N'_i)) \quad (15)$$

$$\hookrightarrow S \in r(C_{K_1}) \quad (16)$$

The new goals (15) and (16) are existed and achieved in the message 3 of the scheme and the assumption (A10).

From the above, the Goal 4: $S \models (U_i \models U_i \xleftrightarrow{SK} S)$ is proved. \square

A Key Distribution Scheme Preventing Collusion Attacks in Ubiquitous Heterogeneous Sensor Networks

Firdous Kausar¹, Sajid Hussain², Jong Hyuk Park³, and Ashraf Masood¹

¹ College of Signals, NUST, Rawalpindi, Pakistan
firdous.imam@gmail.com, ashrafm61@gmail.com

² Jodrey School of Computer Science, Acadia University, Nova Scotia, Canada
sajid.hussain@acadiau.ca

³ Department of Computer Engineering, Kyungnam University, Masan, Korea
parkjonghyuk@gmail.com

Abstract. Random key pre-distribution schemes are vulnerable to collusion attacks. In this paper, we propose a new key management scheme for ubiquitous heterogeneous sensor networks consisting of a small number of powerful high-end \mathcal{H} -sensors and a large number of ordinary low-end \mathcal{L} -sensors. The collusion attack on key pre-distribution scheme mainly takes advantage of the globally applicable keys, which are selected from the same key pool. As a result, in our scheme, after discovering the shared pairwise keys with neighbors, all \mathcal{H} -nodes and \mathcal{L} -nodes destroy their initial key rings and generate new key rings by applying one-way hash function on node's ID and initial key ring. The analysis of proposed scheme shows that even if a large number of nodes are compromised, an adversary can only exploit a small number of keys nearby the compromised nodes, while other keys in the network remain safe. It outperforms the previous random key pre-distribution schemes by considerably reducing the storage requirement, while providing more resiliency against node capture and collusion attacks.

1 Introduction

Wireless sensor networks (WSNs) have attracted wide attention due to their ubiquitous surveillant application. WSNs are formed by a large number of sensor nodes. Each sensor node contains a battery-powered embedded processor and a radio, which enables the nodes to self-organize into a network, communicate with each other and exchange data over wireless links. WSNs are commonly used in ubiquitous and pervasive applications such as military, homeland security, health-care, and industry automation. [1].

An important area of research interest is a general architecture for wide-area sensor networks that seamlessly integrates homogeneous and heterogeneous sensor networks. Heterogeneous sensor networks have different types sensors, with a large number of ordinary sensors in addition to a few powerful sensors. Further, as sensor devices are typically vulnerable to physical compromise and

they have very limited power and processing resources, it is unacceptable to completely trust the results reported from sensor networks, which are deployed outside of controlled environments without proper security.

In order to provide secret communication in a sensor network, shared secret keys are used between communicating nodes to encrypt data. Key establishment protocols are used to set up the shared secrets, but the problem is complicated by the sensor nodes' limited computational capabilities, battery energy, and available memory. Hence, asymmetric cryptography such as RSA or Elliptic Curve cryptography (ECC) is unsuitable for most sensor architectures due to high energy consumption and increased code storage requirements. Several alternative approaches have been developed to perform key management on resource-constrained sensor networks without involving the use of asymmetric cryptography such as single network-wide key, pairwise key establishment, trusted base station, and random key pre-distribution schemes [2].

In random key pre-distribution (RKP) schemes, a large key pool of random symmetric keys is generated along with the key identifiers. All nodes are given a fixed number of keys randomly selected from a key pool. In order to determine whether or not a key is shared, each node broadcasts its keys' identifiers. The neighbors sharing a key associated with one of those identifiers, issue a challenge/response to the source. If two nodes do not share keys directly, they can establish a session key with the help of neighbors with which a key is already shared. It is highly likely that all nodes in the network will share at least one key if the following are carefully considered: a) the network density, b) the size of the key pool, and c) the number of keys pre-configured in each sensor node.

While pre-distributing pairwise keys does protect confidentiality, it still loads nodes with a large number of globally-applicable secrets. By eliminating the eavesdropping attack, the pairwise scheme makes another type of malicious behavior more attractive. As several nodes possess the same keys, any node can make use of them by simply combining the keys obtained from a few nodes, which greatly increases the attacker's chances of sharing keys with other nodes. A collusive attacker can share its pairwise keys between compromised nodes by enabling each node to present multiple 'authenticated' identities to neighboring nodes while escaping detection [3].

An adversary who obtains compromised nodes' keys can inject malicious sensor nodes elsewhere in the network since the pool keys that were obtained are always valid and are used to authenticate each node. As a result, RKP is unable to protect the sensor network against collusion attack. In order to counter the collusion attacks, nodes should discard unused keys from the node's memory after the initialization phase; however, it means that new nodes can no longer join the system after the initial network deployment.

In this paper, we propose a key management scheme based on random key pre-distribution for heterogeneous sensor networks. The proposed scheme is resilient against collusion attack. The rest of the paper is organized as follows. Section 2 provides the related work and Section 3 describes the network and threat model.

In Section 4, the proposed scheme is described in detail. Section 5 gives the results and performance evaluation. Finally, Section 6 concludes the paper.

2 Related Work

Key management for WSNs is a critical issue that has been addressed through many proposed schemes presented in various papers. Eschenauer and Gligor [4] propose a distributed key establishment mechanism that relies on probabilistic key sharing among the nodes of a random graph and uses a shared-key discovery protocol for key establishment. Chan et al. [5] further extended this idea and propose the q -composite key predistribution. This approach allows two sensors to setup a pairwise key only when they share at least q common keys. Chan et al. also developed a random pairwise keys scheme to defeat node capture attacks. Oliveira et al. [6] show how random key predistribution, widely studied in the context of flat networks, can be used to secure communication in hierarchical (cluster-based) protocols such as LEACH [7]. They presented SecLEACH, a protocol for securing node-to-node communication in LEACH-based networks. These and some others [8, 9, 10, 11, 12] efforts have assumed a deployment of homogeneous nodes, and have therefore suggested a balanced distribution of random keys to each of the nodes to achieve security. Most of these schemes suffer from high communication and computation overhead, and/or high storage requirement.

Perrig et al. [13] propose SPINS, a security architecture specifically designed for sensor networks. In SPINS, each sensor node shares a secret key with the base station. Two sensor nodes cannot directly establish a secret key. However, they can use the base station as a trusted third party to set up the secret key.

Blundo et al. [14] propose several schemes that allow any group of t parties to compute a common key, while being secure against collusion between some of them. These schemes focus on saving communication costs, while memory constraints are not placed on group members. When $t = 2$, one of these schemes is actually a special case of Blom's scheme [15].

Availability of some information on the sensors deployment in the field assists to improve the security of the key pre-distribution schemes. Some location-aware schemes are proposed in [16] and [17]. These techniques divide the target field into non-overlapping square areas and randomly deploy the sensors in every area. The exact location of a sensor in any area is unknown, but there is knowledge about the identity of sensors in every area. This information helps to eliminate the dependency of keys between nonadjacent cells.

Du et al. [18] propose the asymmetric pre-distribution (AP) scheme for heterogeneous sensor networks. They consider a small number of powerful high-end sensors and a large number of ordinary low-end sensors. The basic idea of the AP key management scheme is to pre-load a large number of keys in each H-sensor whereas only a small number of keys are pre-loaded in each L-sensor, in order to provide better security with low complexity and significant reduction in storage requirement. Traynor et al. [19] demonstrate that a probabilistic unbalanced

distribution of keys throughout the network that leverages the existence of a small percentage of more capable sensor nodes can not only provide an equal level of security but also reduces the consequences of node compromise. Lu et al. [20] propose a framework for key management schemes in distributed wireless sensor networks with heterogeneous sensor nodes.

3 Network Model

We consider a heterogeneous sensor network (HSN) consisting of a small number of high end (\mathcal{H} -node) and a large number low end (\mathcal{L} -node) sensors. \mathcal{L} -nodes are ordinary sensor nodes with limited computation, communication, and storage capability. \mathcal{H} -nodes, however, are more powerful nodes and have higher computation, communication, energy supply and storage capability than \mathcal{L} -nodes. Further, the HSN includes a base station (BS) that is globally trusted and it receives data from all the nodes; the BS has unlimited resources.

We consider the hierarchical structure of the HSN in which \mathcal{H} -nodes act as cluster heads (CHs). Clustering of sensors enable local data processing, which reduces communication load in the network in order to provide scalable solutions.

We assume that sensor nodes are not mobile. Though they are deployed randomly; once placed at a particular location, they do not tend to move from that location. But it is dynamic in nature as new sensor nodes may be added after network formation or some of the nodes may die down due to energy exhaustion or malfunction. This causes change in neighbor information and overall network topology.

3.1 Threat Model

Sensor networks are often deployed in hostile environments, yet nodes cannot afford expensive tamper-resistant hardware. The threat model is assumed to be an adversary that tries to capture and compromise a number of nodes in the network. Also, there is no unconditional trust on any sensor node. If an adversary compromises a node, the memory of that node is known to the adversary; CHs can also be compromised. The goal of the adversary is to uncover the keys used in the network for secure communication. The nodes can collude with each other by sharing their keys with other attacker nodes.

3.2 Preliminaries

Definition 1. A pseudo-random function is an efficient (deterministic) algorithm which given an h -bit seed, y , and an h -bit argument, x , returns an h -bit string, denoted $f_y(x)$, so that it is infeasible to distinguish the responses of f_y , for a uniformly chosen y , from the responses of a truly random function.

Definition 2. A cryptographically secure one-way hash function H has the following property: for $y = H(x, k)$, 1) given x , it is computationally infeasible to find y without knowing the value of k ; 2) given y and k , it is computationally infeasible to find x .

Table 1. Symbol Definition

| Notation | Definition |
|--------------|--|
| BS | Base Station |
| CH | Cluster Head |
| id_{L_i} | Identity of \mathcal{L} -node i |
| id_{H_i} | Identity of \mathcal{H} -node i |
| N | A random number string |
| R_{L_i} | Set of the keys in \mathcal{L} -node i initial key ring |
| R_{H_i} | Set of the keys in \mathcal{H} -node i initial key ring |
| R'_{L_i} | Set of the keys in \mathcal{L} -node i new/update key ring |
| R'_{H_i} | Set of the keys in \mathcal{H} -node i new/update key ring |
| $K_{X,Y}$ | A shared key between X and Y |
| $\{m\}_K$ | An encryption of message m with key K |
| $MAC_K(msg)$ | MAC calculated using key K |
| \parallel | concatenation symbol |

Definition 3. (*Key Graph*) Let V represent all the nodes in the sensor network. A Key-Sharing graph $G(V,E)$ is constructed in the following manner: For any two nodes i and j in V , there exists an edge between them if and only if nodes i and j have at least one common key in their key ring. Note that $|V| = n$ for a WSN of size n , the key graph $G(V;E)$ is connected if and only if any two nodes i and j belonging to V can reach each other via edge set E only.

For convenience, a summary of notations and symbols used in the paper are given in Table II.

4 Protocol

In this section we describe our key management scheme in detail.

4.1 Initial Deployment

Generate a large key pool P consisting of a S number of random symmetric keys and their ids prior to network deployment. Before deploying the nodes, each node is loaded with its assigned key ring R as follows: each \mathcal{L} -node is pre-loaded with γ number of keys and each \mathcal{H} -node is pre-loaded with ρ number of keys, randomly selected from the key pool without replacement, where $\rho \gg \gamma$. As given in [21], the assigning rules are as follows:

\mathcal{L} -node

for every key $k_i \in P$, where $P = (k_1, k_2, \dots, k_S)$
 compute $z = f_{k_i}(id_{L_x})$
 if $z \equiv 0 \pmod{\left(\frac{S}{\gamma}\right)}$ then
 put k_i into R_{L_x} , the key ring of \mathcal{L} -node.

H-node

for every key $k_i \in P$, where $P = (k_1, k_2, \dots, k_S)$
 compute $z = f_{k_i}(id_{H_x})$
 if $z \equiv 0 \pmod{\left(\frac{S}{\rho}\right)}$ then
 put k_i into R_{H_x} , the key ring of \mathcal{H} -node.

4.2 Cluster Organization Phase

After the initial deployment, nodes enter into the cluster organization phase. Let \mathcal{H} -node H_a broadcasts an advertisement message adv , consisting of its id (id_{H_a}) and N as shown in message 1 of Figure 1. The nearby \mathcal{L} -node L_b upon receiving the adv message, L_b determines whether it shares a common key with H_a as follows: for every key $k_j \in R_{L_b}$, L_b computes $z = f_{k_j}(id_{H_a})$. If $z \equiv 0 \pmod{\left(\frac{S}{\rho}\right)}$, it means that H_a also has a key k_j in its key ring i.e. $R_{H_a} \cap R_{L_b} = k_j$.

As L_b could receive adv broadcast messages from several \mathcal{H} -nodes, it would be possible that L_b shares a common key with more than one \mathcal{H} -node. From these \mathcal{H} -nodes, it will choose the \mathcal{H} -node as its CH with whom it has the best received signal strength and link quality.

L_b sends the join request to the selected CH (say H_a) protected by MAC, using k_j and include the N from CH broadcast (to prevent replay attack), as well as the id of shared key (id_{k_j}) chosen to protect this link (so that the receiving CH knows which key to use to verify the MAC) as shown in message 2 of Figure 1. Both H_a and L_b will generate the shared pairwise key by applying one-way hash function on id_{L_b} and id_{H_a} by using k_j as shown in message 3 of Figure 1.

- 1: $H_a \rightarrow * : id_{H_a}, N$
- 2: $L_b \rightarrow H_a : id_{L_b}, id_{H_a}, id_{k_j}, MAC_{k_j}(id_{L_b} || id_{H_a} || id_{k_j} || N)$
- 3: $K_{H_a, L_b} = H(k_j, id_{H_a} || id_{L_b})$.

Fig. 1. Messages Transferred between sensor nodes and CHs

Direct key discovery phase. After cluster organization phase, \mathcal{L} -nodes learn their neighbors through the exchange of *hello* messages, and then attempt to establish keys with their neighbors. To accomplish this, \mathcal{L} -nodes broadcast *hello* messages.

Consider an \mathcal{L} -node, L_a , it broadcast a *hello* message consisting of its id id_{L_a} . Then, it waits for hello messages from its neighboring \mathcal{L} -nodes. Suppose, it receive hello message from one of its neighbor L_b , it extracts the node id from message i.e. id_{L_b} . For every key $k_j \in R_{L_a}$, L_a computes $z = f_{k_j}(id_{L_b})$. If $z \equiv 0 \pmod{\left(\frac{S}{\gamma}\right)}$, it means that node L_b also has a key k_j in its key ring i.e. $R_{L_a} \cap R_{L_b} = k_j$. After discovering the common key in their key rings, they will generate the shared pairwise key by applying one-way hash function on id_{L_a} and id_{L_b} by using k_j .

$$K_{L_a, L_b} = H(k_j, id_{L_a} || id_{L_b}).$$

If L_a and L_b share more than one common keys in their key rings, the key with the least id would be used to generate the shared pairwise key.

Indirect key discovery phase. \mathcal{L} -nodes gather information about both types of neighbors: 1) nodes with which they share a key, and 2) nodes with which they do not share keys. When the direct key discovery phase ends, the nodes would have discovered the common keys, if any, with their neighbors. \mathcal{L} -nodes use the CH with which keys are already shared to assist it in establishing secure connections with the neighboring \mathcal{L} -nodes with which common keys are not found.

Let \mathcal{L} -nodes L_i and L_j are neighboring nodes in the same cluster; however, they do not share a common key in their key rings, $R_{L_i} \cap R_{L_j} = \phi$. The \mathcal{L} -node L_i , having already established a link with the its CH (H_a), transmits a message to H_a , as shown in Figure 2 requesting to transmit a key with \mathcal{L} -node L_j encrypted with key K_{H_a, L_i} .

The \mathcal{H} -node generates a key k_x and unicasts the message 2 to L_i and message 3 to L_j shown in Figure 2. When L_i (or L_j) receives its message from H_a , it decrypts the message using key K_{H_a, L_i} to get key k_x . Similarly, L_j uses key K_{H_a, L_j} for decrypting the message. Now, L_i and L_j generate the shared pairwise by applying one-way hash function on id_{L_i} and id_{L_j} by using k_x , as shown in message 4.

- 1: $L_i \rightarrow H_a : id_{L_i}, id_{L_j}, N, MAC_{K_{H_a, L_i}}(id_{L_i} || id_{L_j} || N)$
- 2: $H_a \rightarrow L_i : id_{L_i}, id_{L_j}, N, \{k_x\}_{K_{H_a, L_i}}$
- 3: $H_a \rightarrow L_j : id_{L_i}, id_{L_j}, N, \{k_x\}_{K_{H_a, L_j}}$
- 4: $K_{L_i, L_j} = H(k_x, id_{L_i} || id_{L_j}).$

Fig. 2. Messages Transferred between sensor nodes and CHs

4.3 Key Ring Update

After indirect key-discovery phase, all \mathcal{L} -nodes and \mathcal{H} -nodes destroy their initial key rings. Because these key rings have globally applicable secrets which can be used by adversary to launch a collusion attack, we delete these initial key rings.

First, before a node (say L_x) destroys its initial key ring, it generates a new key ring as shown in Figure 3. For every key $k_i \in R_{L_x}$, it generates a new key k'_i by applying one-way hash function on its id (id_{L_x}) and k_i . In this way, it generates a set of new keys from keys in its initial key ring. Further, in order to keep record of the keys in its initial key ring, these newly generated keys are assigned the same ids as that were of the original keys. Then, L_x deletes k_i from its key ring R_{L_x} .

Further, the above procedure is also applied for \mathcal{H} -nodes to update their key rings.

```

procedure keyRingUpdate()
1: for  $\forall k_i \in R_{L_x}$  do
2:    $k'_i = H(k_i, id_{L_x})$ 
3:    $id_{k'_i} = id_{k_i}$ 
4:   delete( $k_i$ )
5: end for

```

Fig. 3. Key Ring Update

4.4 Addition of a New Node

The common key pre-distribution schemes are unable to add new nodes in the network if the initial key rings are deleted from node's memory. As a result, we develop a new solution capable of handling addition of new legitimate \mathcal{L} -nodes beyond the initial deployment, even after the deletion of initial key rings from node's memory.

Suppose new \mathcal{L} -node L_x wants to join a network, it broadcasts a join request consisting of its id (id_{L_x}) and a random number N , as shown in message 1 of Figure 4. Then, it waits for reply from nearby CHs. Let L_x receives a reply message from CH (say H_a). For every key $k_j \in R_{L_x}$, L_x computes $z = f_{k_j}(id_{H_a})$. If for any k_j , $z \equiv 0 \pmod{\frac{S}{\rho}}$, it means that $k_j \in R_{H_a}$, but it is no longer available now because R_{H_a} has been deleted. So, L_x computes the corresponding key i.e. k'_j of H_a 's new key ring R'_{H_a} by applying one-way hash function on id_{H_a} and k_j i.e. $k'_j = H(k_j, id_{H_a})$. Then, L_x sends a message to H_a consisting of its id id_{L_x} , id of k_j ($id_{k_j} = id_{k'_j}$), random number N and MAC is calculated on all these values using k'_j as shown in message 3 of Figure 4. Now, L_x and H_a generate the shared pairwise key by applying one-way hash function on id_{H_a} and id_{L_x} by using k'_j , as shown in message 4.

```

1:  $L_x \rightarrow * : id_{L_x}, N$ 
2:  $H_a \rightarrow L_x : id_{H_a}, N$ 
3:  $L_x \rightarrow H_a : id_{L_x}, MAC_{k'_j}(id_{L_x} || id_{k_j} || N)$ 
4:  $K_{L_x, H_a} = H(k'_j, id_{L_x} || id_{H_a})$ .

```

Fig. 4. New node addition

Then, L_x discovers the shared key with its neighboring \mathcal{L} -nodes by using either direct or indirect key discovery phase, as given above.

5 Analysis

This section analyzes the proposed scheme and explains its features that make this scheme feasible to implement and a better alternative option as compared to the other key pre-distribution schemes.

For any pair of nodes to find a secret key between them, the key sharing graph $G(V, E)$ needs to be connected. Given the size and the density of a network, the objective is to determine the key pool size S , the number of keys assigned to \mathcal{L} -nodes γ , and the number of keys assigned to \mathcal{H} -nodes ρ such that, the graph G is connected with high probability.

For an \mathcal{L} -node, the total possible number of key ring assignments are:

$$\frac{S!}{\gamma!(S - \gamma)!}$$

For an \mathcal{H} -node, the number of possible key ring assignments are:

$$\frac{S!}{\rho!(S - \rho)!}$$

The total number of possible key ring assignments for an \mathcal{L} -node and an \mathcal{H} -node are:

$$\frac{S!}{\gamma!(S - \gamma)!} \times \frac{S!}{\rho!(S - \rho)!}$$

The probability of an \mathcal{L} -node and \mathcal{H} -node with key rings sizes γ and ρ sharing at least one key with each other is given in Equation 1.

$$p = 1 - \frac{(S - \gamma)!(S - \rho)!}{S!(S - \gamma - \rho)!} \tag{1}$$

Figure 5 shows the probability of key sharing among \mathcal{H} -node and \mathcal{L} -node with respect to key pool size. Further, a fixed number of pre-loaded keys are used in \mathcal{H} -nodes, $\rho = 500$; whereas pre-loaded keys for \mathcal{L} -nodes vary as $\gamma = 10, 20, 30$. The graphs show that the pre-loaded keys in \mathcal{L} -nodes can be significantly reduced with acceptable probability of key sharing.

5.1 Security Analysis

We evaluate our key pre-distribution scheme in terms of its resilience against node capture and collusion attack. We would like to investigate when α number of captures nodes are captured, what fraction of the additional communication (i.e. communication among uncaptured nodes) would be compromised?

To compute this fraction, we first compute the probability that any one of the additional communication links is compromised after α nodes are captured. In our analysis, we are considering the links which are secured using a pairwise key computed from the common key shared by the two nodes of this link. We should also notice that during shared key discovery process, two neighboring nodes find the common key in their key rings and use this key to agree upon another random key to secure their communication. Because this new key is generated by applying one-way hash function on common shared key and node ids, the security of this new random key does not directly depend on whether the key rings are broken. Further, the nodes' initial key rings are also deleted

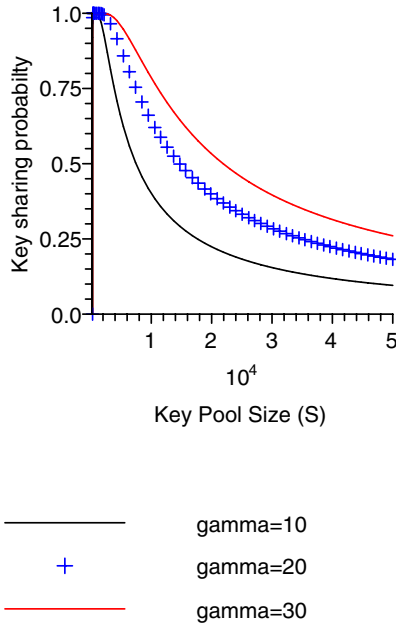


Fig. 5. The Key Sharing Probability

from their memory, after setting up shared pairwise keys with neighbors. As a result, the fraction of communications compromised when α number of nodes being compromised can be given as

$$\frac{\text{number of links in } \alpha \text{ compromised nodes}}{\text{Total number of links}}$$

which means that only those links will be affected which are directly connected with α compromised nodes, while the other links in the network will remain safe. Figure 6 shows the graphs of number of compromised communication links with respect to the number of compromised nodes. We compare our proposed scheme (PS) with basic scheme (EG) [4] and q-composite scheme [5]. The graphs show that as the number of compromised nodes increases, the traditional schemes are severely affected as compared to PS.

Further, in collusion attacks, the adversary takes advantage of the pairwise secret keys stored by each sensor node as these keys are globally applicable secrets and can be used throughout the network, yet ordinary sensors can only communicate with the small fraction of nodes within radio range. So, the adversary can launch a collusion attack by exploiting this lack of communication between nodes and can now share its pairwise keys between compromised nodes, enabling each node to present multiple ‘authenticated’ identities to neighboring nodes, while escaping detection. In proposed scheme, we delete the initial key rings from nodes memory after setting up shared pairwise keys with

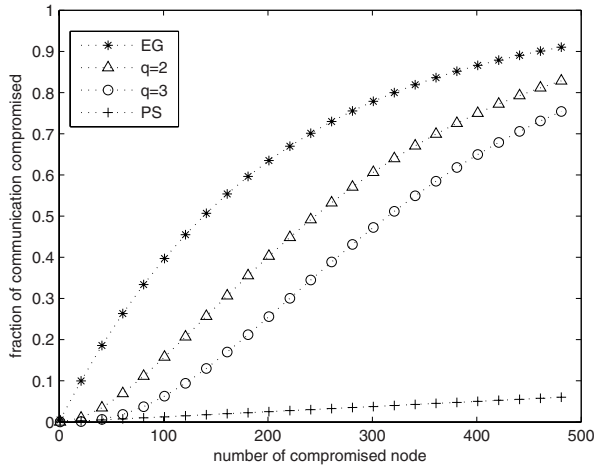


Fig. 6. The Compromising Probability

neighbors. However, nodes generate new key rings from initial key rings by applying one-way hash function on node ids and keys in their initial key rings.

Consider two arbitrary \mathcal{L} -nodes, L_a and L_b , where $R_{L_a} = \{k_1, k_2, \dots, k_\gamma\}$, $R_{L_b} = \{k_1, k_2, \dots, k_\gamma\}$, and $R_{L_a} \cap R_{L_b} = k_i$. As L_a and L_b are not within the communication range of each other, they do not use k_i . After setting up shared pairwise keys with neighbors, both L_a and L_b delete the initial key rings (R_{L_a} and R_{L_b}) and generate the new key rings (say R'_{L_a} and R'_{L_b}) by applying one-way hash function on all the keys in their initial key rings and node ids. As a result, $R'_{L_a} \cap R'_{L_b} = \phi$. Similarly, in α number of compromised nodes, there will be no common key in their new key rings i.e $R'_{L_1} \cap R'_{L_2} \cap \dots \cap R'_{L_\alpha} = \phi$. As no more globally applicable secrets remain in the node's memory, it is not possible by adversary to launch a collusion attack.

6 Conclusion

As secret communication is an important requirement in many sensor network applications, shared secret keys are used between communicating nodes to encrypt data. A key pre-distribution scheme is one of the common solutions for establishing secure communication in sensor networks. Random key pre-distribution schemes are vulnerable to collusion attacks because pre-loading global secrets onto exposed devices can be used in these attacks. In this paper, we propose a key distribution scheme that is robust against the collusion attack. Our scheme provides higher resiliency against node capture and collusion attack by deleting the initial key rings from their memory, after generating the shared pairwise key with neighbors. Further, it allows new nodes to join the system after initialization, even though the initial key ring has been destroyed from the node's memory.

Acknowledgment

This work is in part supported by Higher Education Commission (HEC) Pakistans International Research Support Initiative Programs scholarship given to Firdous Kausar to conduct her research at Acadia University, Canada. Further, we would like to thank National Science and Engineering Research Council (NSERC) Canada for their support in providing RTI and Discovery grants to Dr. Hussain at Acadia University, Canada. This research is also supported by Kyungnam University.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. *IEEE Communications Magazine* (August 2002)
2. Xiao, X., Rayi, V.K., Sun, B., Du, X., Hu, F., Galloway, M.: A survey of key management schemes in wireless sensor networks. *Computer communications* (2007)
3. Moore, T.: A collusion attack on pairwise key predistribution schemes for distributed sensor networks. In: *PERCOMW 2006. Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops*, Washington, DC, USA, p. 251. IEEE Computer Society, Los Alamitos (2006)
4. Eschenauer, L., Gligor, V.D.: A key management scheme for distributed sensor networks. In: *ACM CCS* (2002)
5. Chan, H., Perrig, A., Song, D.: Random key pre-distribution schemes for sensor networks. In: *IEEE Symposium on Security and Privacy*, pp. 197–213 (May 2003)
6. Oliveira, L.B., Wong, H.C., Bern, M., Dahab, R., Loureiro, A.A.F.: Sec leach: A random key distribution solution for securing clustered sensor networks. In: *5th IEEE international symposium on network computing and applications*, pp. 145–154 (2006)
7. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: *IEEE Hawaii Int. Conf. on System Sciences*, pp. 4–7 (2000)
8. Chan, H., Perrig, A., Song, D.: Random key pre-distribution schemes for sensor networks. In: *IEEE Symposium on Research in Security and Privacy* (2003)
9. Zhu, S., Xu, S., Setia, S., Jajodia, S.: Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach. In: *ICNP 2003. 11th IEEE International Conference on Network Protocols* (2003)
10. Pietro, R.D., Mancini, L.V., Mei, A.: Random key assignment secure wireless sensor networks. In: *1st ACM workshop on Security of Ad Hoc and Sensor Networks* (2003)
11. Cheng, Y., Agrawal, D.P.: Efficient pairwise key establishment and management in static wireless sensor networks. In: *Second IEEE International Conference on Mobile ad hoc and Sensor Systems* (2005)
12. Ren, K., Zeng, K., Lou, W.: A new approach for random key pre-distribution in large-scale wireless sensor networks. *Wireless communication and mobile computing* 6(3), 307–318 (2006)
13. Perrig, A., Szewczyk, R., Tygar, J., Victorwen, Culler, D.E.: Spins: Security protocols for sensor networks. In: *Seventh Annual Int'l Conf. on Mobile Computing and Networks* (July 2001)

14. Blundo, C., Santis, A.D., Herzberg, A., Kutten, S., Vaccaro, U., Yung, M.: Perfectly-secure key distribution for dynamic conferences. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 471–486. Springer, Heidelberg (1993)
15. Blom, R.: An optimal class of symmetric key generation systems. In: Beth, T., Cot, N., Ingemarsson, I. (eds.) Advances in Cryptology. LNCS, vol. 209, pp. 335–338. Springer, Heidelberg (1985)
16. Liu, D., Ning, P.: Location-based pairwise key establishments for static sensor networks. In: SASN 2003. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 72–82. ACM Press, New York (2003)
17. Wadaa, A., Olariu, S., Wilson, L., Eltoweissy, M.: Scalable cryptographic key management in wireless sensor networks. In: ICDCSW 2004. Proceedings of the 24th International Conference on Distributed Computing Systems Workshops - W7: EC, Washington, DC, USA, pp. 796–802. IEEE Computer Society, Los Alamitos (2004)
18. Du, X., Xiao, Y., Guizani, M., Chen, H.H.: An effective key management scheme for heterogeneous sensor networks. *Ad Hoc Networks* 5(1), 24–34 (2007)
19. Traynor, P., Kumar, R., Saad, H.B., Cao, G., Porta, T.L.: Establishing pair-wise keys in heterogeneous sensor networks. In: INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings, pp. 1–12 (2006)
20. Lu, K., Qian, Y., Hu, J.: A framework for distributed key management schemes in heterogeneous wireless sensor networks. In: IEEE International Performance Computing and Communications Conference, pp. 513–519 (2006)
21. Pietro, R.D., Mancini, L.V., Mei, A.: Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks. *Wirel. Netw.* 12(6), 709–721 (2006)

Token-Based Authenticated Key Establishment Protocols for Three-Party Communication

Eun-Jun Yoon¹ and Kee-Young Yoo^{2,*}

¹ Faculty of Computer Information, Daegu Polytechnic College,
42 Jinri-2gil (Manchon 3dong San395), Suseong-Gu, Daegu 706-711, South Korea
ejyoon@tpic.ac.kr

² Department of Computer Engineering, Kyungpook National University,
1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, South Korea
Tel.: +82-53-950-5553; Fax: +82-53-957-4846
yook@knu.ac.kr

Abstract. This paper proposes new efficient and secure three-party token-based authenticated key establishment (3TAKE) protocols based on symmetric key cryptosystem to minimize the complexity of symmetric key encryption/decryption operation among all users and fit three-party communication. In 3TAKE, the number of exponentiations among three parties is same or reduced by about 34 ~ 60% and the number of symmetric key encryption/decryption operations among three parties is reduced by about 34 ~ 67% compared with the related protocols, respectively. Furthermore, the number of rounds is one round smaller than the related protocols and the asymmetric key encryption/decryption operations do not need to establish a session key and authenticate between two users and a server.

Keywords: Cryptography, Token, Authentication, Password, Key agreement, Three-party.

1 Introduction

1.1 User Authentication

User authentication is a process that verifies a user's identity to ensure that the person requesting access to the private network is in fact, that person to whom entry is authorized. Generally, there exist three kinds of approaches for user authentication [1,3,4,5]:

1. **Password-based user authentication (“what you know”):** Passwords and PINs are examples of this approach.
2. **Token-based user authentication (“what you have”):** This approach includes physical keys, ATM or smart cards, tokens, mobile devices (cell phones, PDA, sensor nodes) and so on.
3. **Biometric user authentication (“what you are”):** Voice, fingerprints, retinal scans, and keystrokes are included in this approach.

* Corresponding author.

1.2 Authenticated Key Establishment

Authenticated key establishment (AKE) protocols are designed to provide two or more specified entities communicating over an open network with a shared secret key which may subsequently be used to achieve some cryptographic goal such as confidentiality or data integrity [6]. Key establishment may be broadly subdivided into key transport and key agreement that may be employed to establish session keys [2].

- **Key transport protocol:** A key transport protocol is a key establishment technique where one party creates or otherwise obtains a secret value, and securely transfers it to the other(s).
- **Key agreement protocol:** A key agreement protocol is a key establishment technique in which a shared secret is derived by two (or more) parties as a function of information contributed by, or associated with, each of these, (ideally) such that no party can predetermine the resulting value.

1.3 Three-Party Communication Environment

In a three-party (a server and two clients) setting, key transport protocol means that the session key is created by the server and securely transmitted to these two clients, and key agreement protocol means that both clients contribute information to derive the common session key.

Recently some researches proposed three-party AKE protocols. However, these protocols are insecure some attacks and inefficiently designed because of performing many symmetric key encryption/decryption operations. Gong, Lomas, Needham, and Saltzer [7] proposed a protocol, called GLNS protocol, in a three-party setting in which two users establish a session key through an authentication server. Timestamps are used in the protocol to guarantee message freshness. By using nonces and confounders, the protocol is successful in generating a large search space to resist off-line password guessing attacks. Many protocols [8,9,10,11,12,13,16] have been addressed to discuss this problem.

1.4 Our Contributions

This paper proposes new efficient and secure three-party token-based authenticated key establishment (3TAKE) protocol based on symmetric key cryptosystem to minimize the complexity of symmetric key encryption/decryption operation among all users and fit three-party communication. The proposed 3TAKE protocols have several important features as follows:

- The proposed 3TAKE protocols are designed to reduce the computation cost of each participant by using the small number of exponentiations.
- The proposed 3TAKE protocols achieve cryptographic goals only using symmetric key cryptosystems, exponentiations and collision-free one-way hash functions as main cryptographic operations without additional requirements such as using server's public key, digital signatures, and so on.

- The proposed 3TAKE protocols use the bitwise exclusive-OR operation and symmetric key cryptosystems to authenticate each other among parties. Additionally, this allows the protocols simply prevent off-line password guessing attack.
- The proposed 3TAKE protocols not only are secure against well-known cryptographical attacks but also provide perfect forward secrecy.

In 3TAKE, the number of exponentiations among three parties is same or reduced by about 34 ~ 60% and the number of symmetric key encryption/decryption operations among three parties is reduced by about 34 ~ 67% compared with the related protocols, respectively. Furthermore, the number of rounds is smaller one round than the related protocols and the asymmetric key encryption/decryption operations do not need to establish a session key and authenticate between two users and a server.

The remainder of this paper is organized as follows: In the next section, we provide preliminary information of 3TAKE. The proposed 3TAKE protocol is presented in Section 3, while Sections 4 and 5 discuss the security and efficiency of the proposed 3TAKE protocol. The Conclusion is given in Section 6.

2 Preliminary Information

This section summarizes the underlying primitives used throughout this paper.

2.1 Notations

Some of the notations used in the proposed 3TAKE are defined as follows:

- A, B, S : Two users and remote server, respectively.
- ID_A, pw_A : User A 's identifier and password, respectively.
- ID_B, pw_B : User B 's identifier and password, respectively.
- x : S 's strong secret key.
- r_i : Fresh random nonce.
- p : Large prime (usually at least 1024 or 2048 bits).
- q : Relatively small prime (typically of 160 bits) with $q|p - 1$.
- Z_q : Subgroup of order q of Z_p^* .
- g : Generator g of Z_q .
- a, b : Session-independent random exponents $\in [1, q - 1]$ chosen by A and B , respectively.
- sk : Shared fresh session key computed by A and B .
- $E_{v_i}(M)$: Symmetric key encryption of message M by using secret key v_i .
- $h(\cdot), f(\cdot)$: Collision resistant secure one-way hash function with an output size of 512 bits, e.g. SHA-512.
- \oplus : Bit-wise exclusive-OR (XOR) operation.

2.2 Review of Related Protocols

This subsection briefly reviews the related three-party AKE protocols [11,12,9] and then point out the efficiency problems of their protocols.

(1) *LSH's three-party key agreement protocol [11]*: The following protocol shows LSH's three-party password-based authenticated key agreement protocol. LSH's protocol requires totally 2 times asymmetric encryption and 2 times asymmetric decryption.

- K_S : S 's public key.

1. $A \rightarrow B: ID_A, \{r_A, g^a, pw_A\}_{K_S}$
2. $B \rightarrow S: ID_A, \{r_A, g^a, pw_A\}_{K_S}, \{r_B, g^b, pw_B\}_{K_S}$
3. $S \rightarrow B: E_{r_A}(B, g^b), E_{r_B}(A, g^a)$
4. $B \rightarrow A: E_{r_A}(B, g^b), E_{sk}(h(flow1), Nonce_B)$
5. $A \rightarrow B: Nonce_B$

(2) *LSSH's three-party key agreement protocol [12]*: The following protocol shows LSSH's three-party password-based authenticated key agreement protocol. LSSH's protocol requires totally 7 rounds and six exponentiation operations.

- S_1, S_2 : Session independent random exponents chosen by S .
 - $K_{A,S}$: Shared session key computed by A and S .
 - $K_{B,S}$: Shared session key computed by B and S .

1. $A \rightarrow S: ID_A, ID_B$
2. $S \rightarrow A: E_{pw_A}(g^{S_1}), E_{pw_B}(g^{S_2})$
3. $A \rightarrow B: ID_A, g^a, f_{K_{A,S}}(ID_A, ID_B, g^{S_1}), E_{pw_B}(g^{S_2})$
4. $B \rightarrow S: g^a, f_{K_{A,S}}(ID_A, ID_B, g^{S_1}), g^b, f_{K_{B,S}}(ID_A, ID_B, g^{S_2})$
5. $S \rightarrow B: f_{K_{B,S}}(ID_A, ID_B, g^a, g^b), f_{K_{A,S}}(ID_A, ID_B, g^b, g^a)$
6. $B \rightarrow A: g^b, f_{K_{A,S}}(ID_A, ID_B, g^b, g^a), f_{sk}(ID_A, ID_B, g^a)$
7. $A \rightarrow B: f_{sk}(ID_A, ID_B, g^b)$

(3) *Juang's three-party key agreement protocol [9]*: The following protocol shows Juang's three-party password-based authenticated key agreement protocol. Juang's protocol requires totally 6 times symmetric encryption and 6 times symmetric decryption.

- Shared Information: $h(\cdot), p, q, g$.
 - Information held by User A : $ID_A, pw_A, \text{Token}(v_A = h(ID_A, x), h(\cdot), p, q, g)$.
 - Information held by User B : $ID_B, pw_B, \text{Token}(v_B = h(ID_B, x), h(\cdot), p, q, g)$.
 - Information held by Remote Server S : x .

1. $A \rightarrow B: r_A, ID_A, E_{v_A}(g^a, h(ID_A, ID_B, r_A))$
2. $B \rightarrow S: r_A, r_B, ID_A, ID_B, E_{v_A}(g^a, h(ID_A, ID_B, r_A)), E_{v_B}(g^b, h(ID_A, ID_B, r_B))$
3. $S \rightarrow B: E_{v_B}(g^a, r_A, r_B + 1), E_{v_A}(g^b, r_B, r_A + 1)$
4. $B \rightarrow A: E_{sk}(r_A + 1), E_{v_A}(g^b, r_B, r_A + 1)$
5. $A \rightarrow B: E_{sk}(r_B + 1)$

3 Proposed Three-Party TAKE Protocol

This section presents three-party token-based authenticated key establishment (3TAKE) protocol. 3TAKE protocol is composed of two protocols, which are key transport (3TAKT) and key agreement (3TAKA).

3.1 Three-Party Key Transport

This subsection proposes three-party token-based key transport (3TAKT) protocol. 3TAKT protocol is composed of two phases, which are the registration phase and the session key transport phase.

Registration Phase: User U_i freely chooses his/her ID_i , password pw_i and random nonce n_i , and interactively submits $\{ID_i, pw_i \oplus n_i\}$ to the remote server S . These private data must be sent in person or over a secure channel. U_i also imprints his/her biometric impression at the sensor, and then S performs the following operations:

- R.1: Computes $v_i = h(ID_i, x)$, $w_i = v_i \oplus h(pw_i \oplus n_i, S_i)$ and $x_i = h(v_i)$, where S_i is the extracted biometric template of U_i .
- R.2: Writes the secure information $\{w_i, x_i, S_i, h(\cdot)\}$ to the memory of U_i 's token and issue the token to U_i through a secure channel.

Upon receiving the token, U_i enters n_i into his/her token.

Key Transport Phase: Figure 1 shows the session key transport phase of 3TAKT protocol. The session key transport phase performs as follows:

In the session key transport phase, after getting the token from S , A can use it when he/she securely communicates with B . If A wants to negotiate a session key with B , he/she opens the login application software, enters ID_A and pw_A , and imprints biometric at the sensor. For simplicity, we omit the verification process to check $h(v_A)$ with the stored x_A from this phase. If U_A is successfully verified by his/her biometric, A 's token performs the following operations:

- S.1 $A \rightarrow S$: $ID_A, E_{v_A}(ID_A, ID_B, r_A)$
 A 's token computes $v_A = w_A \oplus h(pw_A, n_A)$, chooses a random nonce r_A , and sends his/her ID_A and the encrypted message $E_{v_A}(ID_A, ID_B, r_A)$ to S .

- S.2 $S \rightarrow B$: $E_{v_B}(ID_B, ID_A, r_A \oplus sk, sk)$

Upon receiving the message in Step S.1, S first computes $v_A = h(ID_A, x)$ using his/her master secret key x and then decrypts the received message $E_{v_A}(ID_A, ID_B, r_A)$. Then, S checks if the message contain the A 's identity ID_A . If the identity is not valid, S rejects this request. If ID_A is valid, S computes $v_B = h(ID_B, x)$ and generates the session key sk for A and B . Finally, S sends the encrypted message $E_{v_B}(ID_B, ID_A, r_A \oplus sk, sk)$ to B .

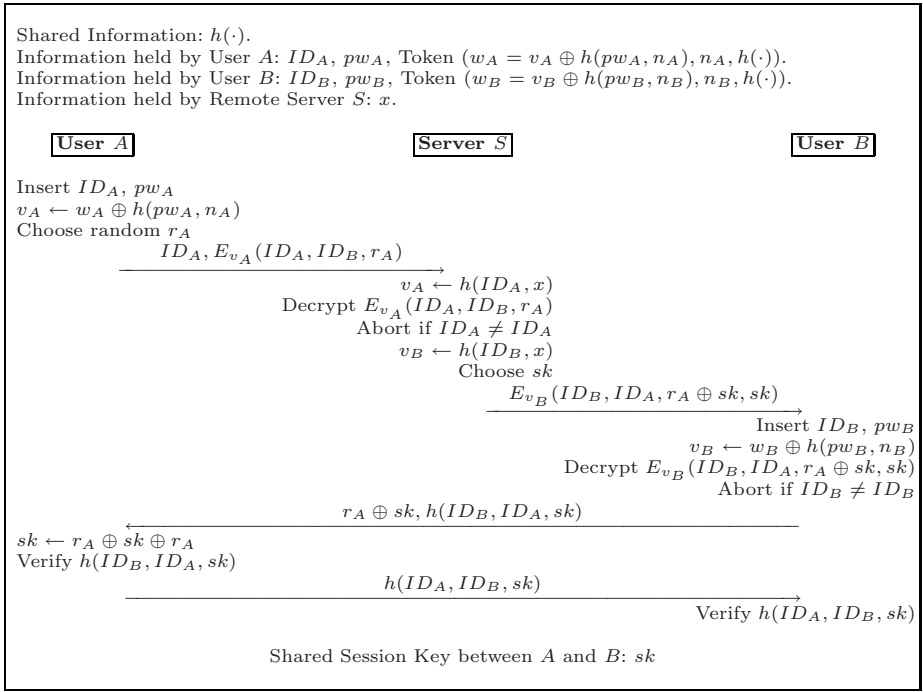


Fig. 1. 3TAKT protocol

S.3 $B \rightarrow A: r_A \oplus sk, h(ID_B, ID_A, sk)$

Upon receiving the message in Step S.2, B inputs his/her identity ID_B and password pw_B to his/her token. Then, B 's token computes $v_B = w_B \oplus h(pw_B, n_B)$ and decrypts the received message $E_{v_B}(ID_B, ID_A, r_A \oplus sk, sk)$. Then, B checks if the message contain his/her identity ID_B . If the identity is not valid, B rejects this request. If ID_B is valid, B computes $h(ID_B, ID_A, sk)$ and sends it with $r_A \oplus sk$ to A .

S.4 $A \rightarrow B: h(ID_A, ID_B, sk)$

After receiving the message in Step S.3, A extracts shared session key sk by computing $r_A \oplus sk \oplus r_A$ and checks if the hash value $h(ID_B, ID_A, sk)$ is correct. If yes, A computes and sends $h(ID_A, ID_B, sk)$ back to B .

S.5 After receiving the message in Step S.4, B checks if the hash value $h(ID_A, ID_B, sk)$ is correct. Then A and B can use the shared secret session key sk in private communication soon.

3.2 Three-Party Key Agreement

This subsection proposes three-party token-based key agreement (3TAKA) protocol. 3TAKA protocol is composed of two phases, which are the registration phase and the session key transport phase.

Registration Phase: The registration phase is same as 3TAKT.

Key Agreement Phase: Figure 2 shows the session key agreement phase of 3TAKT protocol. The session key agreement phase performs as follows:

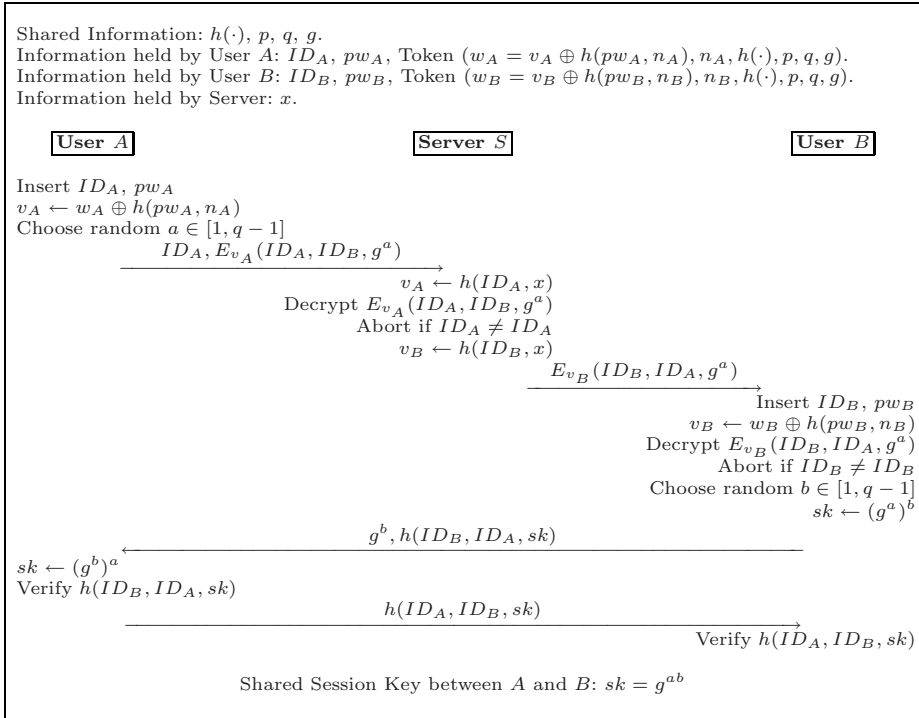


Fig. 2. 3TAKA protocol

In the session key agreement phase, after getting the token from S , A can use it when he/she securely communicates with B . If A wants to negotiate a session key with B , he/she opens the login application software, enters ID_A and pw_A . Then A 's token performs the following operations. For simplicity, we omit $(\text{mod } p)$ from expressions.

- S.1 $A \rightarrow S: ID_A, E_{v_A}(ID_A, ID_B, g^a)$
 User A 's token computes $v_A = w_A \oplus pw_A$, chooses a random number $a \in [1, q - 1]$, and computes g^a . Then, A sends his/her ID_A and the encrypted message $E_{v_A}(ID_A, ID_B, g^a)$ to S .
- S.2 $S \rightarrow B: E_{v_B}(ID_B, ID_A, g^b)$
 Upon receiving the message in S.1, S first computes $v_A = h(ID_A, x)$ using his/her master secret key x and then decrypts the received message $E_{v_A}(ID_A, ID_B, g^a)$. Then, S checks if the message contain the A 's identity

ID_A . If the identity is not valid, S rejects this request. If ID_A is valid, S computes $v_B = h(ID_B, x)$ and sends the encrypted message $E_{v_B}(ID_B, ID_A, g^a)$ to B .

S.3 $B \rightarrow A: g^b, h(ID_B, ID_A, g^a, sk)$

Upon receiving the message in S.2, B inputs his/her identity ID_B and password pw_B to his/her token. Then, B 's token computes $v_B = w_B \oplus h(pw_B, n_B)$ and decrypts the received message $E_{v_B}(ID_B, ID_A, g^b)$. Then, B checks if the message contain his identity ID_B . If the identity is not valid, B rejects this request. If ID_B is valid, B chooses a random number $b \in [1, q - 1]$, and computes g^b and the shared session key $sk = (g^a)^b = g^{ab}$. Finally, B sends g^b and $h(ID_B, ID_A, g^a, sk)$ to A .

S.4 $A \rightarrow B: h(ID_A, ID_B, g^b, sk)$

After receiving the message in S.3, A computes the shared session key $sk = (g^b)^a = g^{ab}$ and checks if the hash value $h(ID_B, ID_A, g^a, sk)$ is correct. If yes, A computes and sends $h(ID_A, ID_B, g^b, sk)$ back to B .

S.5 After receiving the message in S.4, B checks if the hash value $h(ID_A, ID_B, g^b, sk)$ is correct. Then A and B can use the shared secret session key $sk = g^{ab}$ in private communication soon.

4 Security Analysis

This section provides the proof of correctness of the proposed 3TAKE. Here, four security properties [18][19][3]: guessing attacks, replay attacks, mutual authentication and perfect forward secrecy, would be considered for 3TAKE. Under the definitions of Section 2, the following theorems are used to analyze the three security properties in 3TAKE protocols.

Theorem 1. *The proposed 3TAKE protocol can resist guessing attacks.*

Proof. The undetectable on-line password guessing attack will fail, since after Step S.2 of 3TAKE, S can authenticate A . The off-line password guessing attack will not work against 3TAKT since the password pw_A is only used for protecting the corresponding token, and no verifiable information is encrypted by passwords. Also, the secret $w_A = v_A \oplus h(pw_A, n_A)$ is stored in A 's token. Only the legal user A has his/her password pw_A can compute the secret $v_A = w_A \oplus h(pw_A, n_A)$ and then use his/her token.

Therefore, the proposed 3TAKE protocol can resist guessing attacks.

Theorem 2. *The proposed 3TAKE protocol can resist replay attacks.*

Proof. In the proposed 3TAKT, the replay attacks fail because the freshness of the messages transmitted in the session key transport phase is provided by the random nonce r_A and session key sk . Only A and B , who can get the session key sk , can embed the session key sk in the hashed messages $h(ID_B, ID_A, r_A, sk)$ generated by A of Step S.4 and $h(ID_A, ID_B, sk)$ generated by B of Step S.5, respectively.

In the proposed 3TAKA, the replay attacks fail because the freshness of the messages transmitted in the session key agreement phase is provided by the exponents a and b . Except for A , only B who can compute the session key sk can embed the nonce g^a and the session key sk generated by A in the hashed message $h(ID_B, ID_A, g^a, sk)$ of Step S.4. Except for B , only A who can compute the session key sk can embed the nonce g^b and the session key sk generated by B in the hashed message $h(ID_A, ID_B, g^b, sk)$ of Step S.5.

Therefore, the proposed 3TAKE protocol can resist replay attacks.

Theorem 3. *The proposed 3TAKE protocol provides the mutual authentication.*

Proof. In 3TAKT protocol, the goal of mutual authentication is to generate an agreed session key sk between A and B for i -th session. In Step S.3 of the session key transport phase, after B receiving the encrypted message $E_{v_B}(ID_B, ID_A, r_A)$ from S , he/she will check if the encrypted message contains the identity ID_B . Since the identity ID_B is encrypted by the secret key v_B shared between S and B , B will believe the i -th random value r_A was originally sent from A , verified by the trusted server S in Step S.2 and then sent to him/her. B then can compute the session key sk . In Step S.4, after A receiving the encrypted message r_B and $h(ID_B, ID_A, r_A, sk)$ from B , he/she will check if the encrypted message contains the random value r_A and the session key sk . Since the hashed message included r_A and sk , A will believe $h(ID_B, ID_A, r_A, sk)$ was originally sent from B , verified by the trusted server S in Step S.2 and then sent to him/her.

In 3TAKA protocol, the goal of mutual authentication is to generate an agreed session key sk between A and B for i -th session. In Step S.3 of the session key agreement phase, after B receiving the encrypted message $E_{v_B}(ID_B, ID_A, g^a)$ from S , he will check if the encrypted message contains the identity ID_B . Since the identity ID_B is encrypted by the secret key v_B shared between S and B , B will believe the i -th random value g^a was originally sent from A , verified by the trusted server S in Step S.2 and then sent to him/her. B then can compute the session key sk . In Step S.4, after A receiving the encrypted message g^b and $h(ID_B, ID_A, g^a, sk)$ from B , he/she will check if the encrypted message contains the random value g^a and the session key sk . Since the hashed message included the shared session key sk between A and B , A will believe the i -th random value g^b was originally sent from B , verified by the trusted server S in Step S.2 and then sent to him/her. A then can compute the session key sk .

Therefore, the proposed 3TAKE protocol provides the mutual authentication.

Theorem 4. *The proposed 3TAKA protocol provides perfect forward secrecy.*

Proof. A disclosed long-lived secret key v_A , v_B or x cannot derive the session key $sk = g^{ab}$ used before because without getting the used random exponents a and b , nobody can compute the used session key sk . If an attacker wiretaps all conversations of the medium and derives some used random values g^a and g^b , he/she could not compute the used session key sk . This problem is the Diffie-Hellman key exchange algorithm.

Therefore, the proposed 3TAKA protocol provides perfect forward secrecy.

5 Efficiency Analysis

This section discusses the efficiency of newly proposed 3TAKT and 3TAKA protocols.

5.1 Efficiency of 3TAKT Protocol

In recent years, a variety of protocols, which belong to three-part authenticated key transport (3AKT) protocol, have been proposed. This subsection compares some well-known traditional 3AKT protocols including the optimal GLNS protocol [7], the improved K1P protocol [14], the extension of Otway-Rees protocol [3], and KTAP-1 of Yeh [15], with our newly proposed 3TAKT protocol. Optimal GLNS protocol improved the performance of their original GLNS protocol [7] and improved K1P [14] improved three-way K1P [16] which is vulnerable to a straight replay attacks.

We focus on several items such as the number of rounds, the number of random numbers, the number of symmetric encryption/decryption operations, and the number of asymmetric encryption/decryption operations. We ignore other comparisons like the total amount of data transferred because these items are varying for different security levels. Table 1 shows the comparison results.

In Table 1, we can find that proposed 3TAKT is the most efficient in number of rounds, number of random numbers, and other computational costs. That is, in 3TAKT, the number of symmetric key encryption/decryption operations among three parties is reduced by about 34 ~ 67% compared with the related protocols. Furthermore, the number of rounds is smaller one round than the related protocols and the asymmetric key encryption/decryption operations do not need to transport a session key and authenticate between two users and a server.

Table 1. Comparison of efficiency with related 3AKT protocols

| Computations costs | Optimal GLNS (1995) | Extension of OR (1997) | Improved K1P (1999) | KTAP-1 (2003) | 3TAKT |
|-----------------------------------|---------------------------|------------------------------|---------------------------|------------------|--------------|
| # of asymmetric enc/decryption | 2/2 | 0 | 2/2 | 2/2 | 0 |
| # of symmetric enc/decryption | 4/4 | 6/6 | 4/4 | 3/3 | 2/2 |
| # of random numbers | 10 | 3 | 5 | 4 | 3 |
| # of rounds | 5 | 5 | 5 | 5 | 4 |

5.2 Efficiency of 3TAKA Protocol

In recent years, a variety of protocols, which belong to three-part authenticated key agreement (3AKA) protocol, have been proposed. This subsection compares some well-known traditional 3AKA protocols including STW [13], LSH [11],

LSSH [12], ECC [17], KAAP-1 [15], and Juang [9], with our newly proposed 3TAKA protocol. Table 2 shows the comparison results.

In Table 2, we can find that proposed 3TAKA protocol is the most efficient in number of rounds, number of random numbers, and other computational costs. That is, in 3TAKA, the number of exponentiations among three parties is same or reduced by about 34 ~ 60% and the number of symmetric key encryption/decryption operations among three parties is reduced by about 34 ~ 67% compared with the related protocols, respectively. Furthermore, the number of rounds is smaller one round than the related protocols and the asymmetric key encryption/decryption operations do not need to establish a session key and authenticate between two users and a server.

Table 2. Comparison of efficiency with related 3AKA protocols

| Computations costs | STW (1995) | LSH (2000) | LSSH (2001) | KAAP-1 (2003) | ECC (2004) | Juang (2004) | 3TAKA |
|--------------------------------|---------------|---------------|----------------|------------------|---------------|-----------------|-------|
| # of asymmetric enc/decryption | 0 | 2/2 | 0 | 2/2 | 0 | 0 | 0 |
| # of symmetric enc/decryption | 0 | 3/3 | 2/2 | 3/3 | 2/2 | 6/6 | 2/2 |
| # of exponentials | 6 | 8 | 10 | 4 | 10 | 4 | 4 |
| # of hash functions | 0 | 2 | 10 | 0 | 16 | 8 | 4 |
| # of random numbers | 3 | 5 | 4 | 3 | 5 | 4 | 2 |
| # of rounds | 5 | 5 | 5 | 5 | 5 | 5 | 4 |

6 Conclusions

This paper proposed new efficient and secure three-party token-based authenticated key establishment (3TAKE) protocol based on symmetric key cryptosystem to minimize the complexity of symmetric key encryption/decryption operation among all users and fit three-party communication. In 3TAKE, the number of exponentiations among three parties is same or reduced by about 34 ~ 60% and the number of symmetric key encryption/decryption operations among three parties is reduced by about 34 ~ 67% compared with the related protocols, respectively. Furthermore, the number of rounds is smaller one round than the related protocols and the asymmetric key encryption/decryption operations do not need to establish a session key and authenticate between two users and a server.

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. This research was supported by the MIC of Korea, under the ITRC support program supervised by the IITA (IITA-2006-C1090-0603-0026).

References

1. Shneier, B.: Applied Cryptography, 2nd edn. John Wiley & Sons, Inc., Chichester (1996)
2. Boyd, C., Mathuria, A.: Protocols for Authentication and Key Establishment. Springer, Heidelberg (2003)
3. Menezes, A.J., Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptograph. CRC Press, New York (1997)
4. Mao, W.: Modern Cryptography Theory & Practice. Prentice Hall, Englewood Cliffs (2004)
5. Stinson, D.: Cryptography Theory and Practice, 2nd edn. Chapman & Hall/CRC (2002)
6. Blake-Wilson, S., Menezes, A.: Authenticated Diffie-Hellman Key Agreement Protocols. In: Tavares, S., Meijer, H. (eds.) SAC 1998. LNCS, vol. 1556, pp. 339–361. Springer, Heidelberg (1999)
7. Gong, L., Lomas, M., Needham, R., Saltzer, J.: Protecting Poorly Chosen Secrets from Guessing Attacks. IEEE Journal on Selected Areas in Communications 11(5), 648–656 (1993)
8. Gong, L.: Optimal Authentication Protocols Resistant to Password Guessing Attacks. In: Proc. of the 8th IEEE Computer Security Foundation Workshop, pp. 24–29 (1995)
9. Juang, W.S.: Efficient Three-Party Key Exchange using Smart Cards. IEEE Transactions on Consumer Electronics 50(2), 619–624 (2004)
10. Keung, S., Siu, K.: Efficient Protocols Secure Against Guessing and Replay Attacks. In: Proc. of the Fourth International Conference on Computer Communications and Networks, pp. 105–112 (1995)
11. Lin, C., Sun, H., Hwang, T.: Three-party Encrypted Key Exchange: Attacks and a Solution. ACM Operating Systems Review 34(4), 12–20 (2000)
12. Lin, C., Sun, H., Steiner, M., Hwang, T.: Three-party Encrypted Key Exchange Without Server Public-Keys. IEEE Communication Letters 5(12), 497–499 (2001)
13. Steiner, M., Tsudik, G., Waidner, M.: Refinement and Extension of Encrypted Key Exchange. ACM Operating Systems Review 29(3), 22–30 (1995)
14. Kwon, T., Kang, M., Jung, S., Song, J.: An Improvement of the Password based Authentication Protocol (K1P) on Security against Replay Attacks. IEICE Transactions on Communications E82-B(7), 991–997 (1999)
15. Yeh, H.T.: User Authentication and Key Exchange Protocols Suitable for Diverse Circumstances, Ph.D. Thesis, Southern Taiwan University of Technology, Taiwan, pp. 1–82 (2003)
16. Kwon, T., Kang, M., Song, J.: An Adaptable and Reliable Authentication Protocol for Communication Networks. In: Proc. of IEEE INFOCOM 1997, pp. 737–744 (1997)
17. Chang, C., Chang, Y.: A Novel Three-party Encrypted Key Exchange Protocol. Computer Standards & Interfaces 26(5), 471–476 (2004)
18. Lin, C.L., Hwang, T.: A Password Authentication Scheme with Secure Password Updating. Computers & Security 22(1), 68–72 (2003)
19. Liao, I.E., Lee, C.C., Hwang, M.S.: A Password Authentication Scheme over Insecure Networks. Journal of Computer and System Sciences 72(4), 727–740 (2006)

Two Approaches on Pairwise Key Path Establishment for Sensor Networks*

Ping Li¹, Yaping Lin², and Jiaying Wu¹

¹ School of Computer and Telecommunications, Changsha university of Science and Technology, 410076, Changsha, Hunan, China

² College of Software, Hunan University, 410072, Changsha, Hunan, China
lping9188@163.com, yplin@hnu.cn, jiaying528@163.com

Abstract. Developments on WSN technologies have made applications of ubiquitous computing available in recent a few years. The properties of weak connectivity in subsection based on hypercube model are addressed, for purpose of achieving inner-area pairwise key establishment. Also a clustering scheme for inter-area path establishment is proposed, based on the contribution of our presented protocol for key information exchange. Security analysis and performance issue are also addressed.

Keywords: pairwise key, sensor networks, ubiquitous computing, hypercube, security.

1 Introduction

More and more research attentions have been attracted on the security issue in wireless sensor networks (WSN) because of their tremendous applications available in military as well as civilian areas^[1]. At the same time, rapid development on relative technologies of WSN have made applications of ubiquitous computing available in recent a few years. Security schemes of pairwise key establishment, which enable sensors to communicate with each other securely, play a fundamental role in research on security issue in wireless sensor networks^[2].

One of the most important issues on pairwise key establishment is key-pre-distribution phase. Two kinds of pre-distribution schemes are available, centralized and localized schemes according to information pre-loaded in each sensors. With respect to the former, Eeschnaure et al^[4] presented a probabilistic key pre-distribution scheme. For each node in this scheme, m keys are randomly selected from the key pool S and stored into the node's memory so that any two sensors have a certain probability of sharing at least one common key. Based on the contributions made by [5], a lot of attention has focused on polynomial based key pre-distribution.

* Supported by Scientific Research Fund of Hu'nan Provincial Education Department of China under Grant No. 06B005.

That is, the key setup server randomly generates a t -degree bivariate polynomial $f(x,y)$ over a finite field F_q . Notes that for any variables x and y , $f(x,y)=f(y,x)$ is always held. For any two nodes i and j , the key server computes two shares of $f(x,y)$, denoted as $f(i,y)$ and $f(j,y)$, for the two nodes respectively. Thus they can compute the common key $f(i,j)$ directly.

However, those approaches have some limitations. For the centralized schemes such as probabilistic and polynomial-based schemes^{[4][6]}, a small number of compromised sensors may reveal a large fraction of pairwise keys shared by non-compromised sensors. Polynomial-based scheme can only tolerate no more than t compromised nodes, while the value of t is limited due to the memory constrains of sensor nodes^[5].

As security challenges arise in centralized schemes, localized schemes have become research focus. Liu et al^[7] developed a general framework of polynomial pool-based key pre-distribution and proposed two instantiations, a random subset assignment scheme and a hypercube-based assignment scheme for key pre-distribution. Liu et al^[8] also presented a location-aware deployment model, and developed corresponding pairwise key pre-distribution scheme, using location information. The scheme took advantages of the observation that in static sensor networks, although it is difficult to precisely pinpoint sensors' positions, it is often possible to approximately determine their locations.

One the other hand, the possibility to establish direct key in the hypercube-based assignment is not perfect. Furthermore, [7] makes an assumption that a node's signal range can cover the entire network. That implicitly means all the other nodes in a network are direct neighbors for a given nodes. The location-based scheme can achieve better performance due to the explicit usage of location information, while the polynomial pool is fairly small, as sensors expected in the same area have common polynomial shares.

In this paper, we develop two kinds of pairwise key establishment to address above problems in sensor networks. The contribution of this paper is two-fold. First, we model a local network with densely distributed nodes as a hypercube, inspect properties of k -dimensional weak-connectivity in subsection of hypercube model, and develop an effective scheme on pairwise key establishment for inner-area nodes. The resulting scheme guarantees any two sensors appropriating the connectivity requirements to establish pairwise key even though a large number of nodes are compromised or out of communication. Second, a clustering scheme for inter-area path establishment is proposed, based on the contribution of our presented protocol for key information exchange, focusing on networks of large scale with huge number of nodes in a wide deployment area. Our analysis indicates that presented schemes provide nice performance on isolated connected graph clustering as well as key path establishment in inner-area communications.

The rest of this paper is organized as follows. After a brief description on hypercube-based pairwise key establishment in Section 2, Section 3 inspects properties of k -dimensional weak-connectivity in subsection of hypercube model, and presents inner-area scheme on pairwise key establishment. Section 4 describes a clustering scheme as well as a security protocol for pairwise key path establishment. Section 5 analyzes performance of presented schemes, before Section 6 concludes this paper.

2 Hypercube-Based Pairwise Key Establishment Schemes

Given a total of N sensor nodes in the network, this scheme constructs an n -dimensional hypercube with m^{n-1} bivariate polynomials arranged for each dimension j , $\{f_{\langle i_1, \dots, i_{n-1} \rangle}^j(x, y) \mid 0 \leq i_1, i_2, \dots, i_{n-1} < m\}$, where $m = \lceil \sqrt[n]{N} \rceil$. A node's coordinate is encoded in the hypercube into a single-valued node ID. Every valid coordinate in the hypercube is first converted into n l -bit binary strings (one for each dimension) where $l = \lceil \log_2 m \rceil$. Each ID j is expressed as $\langle j_1, j_2, \dots, j_n \rangle$, where j_i is called the sub-index of ID j in dimension i , which also represents the i^{th} l bits of j .

The key setup server randomly generates $n \cdot m^{n-1}$ bivariate t -degree polynomial pool over a finite field F_q , denoted as

$$F = \{ f_{\langle i_1, i_2, \dots, i_{n-1} \rangle}^i(x, y) \mid 0 \leq i_1, i_2, \dots, i_{n-1} \leq n, 1 \leq j \leq n \}.$$

For each node, the setup server then selects an unoccupied coordinate (j_1, j_2, \dots, j_n) in the n -dimensional space and assigns it to this node. The setup server then distributes the following polynomial shares:

$$\{ f_{\langle j_2, \dots, j_n \rangle}^1(x, y), f_{\langle j_1, j_3, \dots, j_n \rangle}^2(x, y), \dots, f_{\langle j_1, j_2, \dots, j_{n-1} \rangle}^n(x, y) \}$$

to this sensor node.

To establish a pairwise key with node j , node i checks whether they have the same sub-index in $n-1$ dimensions. That is, if both the nodes are logical neighbors in the hypercube, expressed as $d_h(i, j) = 1$, they share a common polynomial, and thus they can establish a direct key. Otherwise, they need to go through path discovery to establish indirect key. If there are no compromised nodes and any two nodes can communicate with each other, the node assignment algorithm guarantees at least one key path that can be used to establish a session key between any two nodes. Alternative key paths are created by dynamic key path discovery in case that intermediate nodes have been compromised. Please refer to [7] for details.

3 Inner-area Pairwise Key Path Establishment

In this Section we consider a simpler situation: Assume that a fairly large number of sensor nodes are densely distributed in a small area. We believe that only in that kind of situation does it make sense to apply the properties of basic hypercube model on pairwise key establishment. In this Section, we mainly inspect the weak connectivity issue on hypercube, and present a scheme on inner-area pairwise key establishment.

3.1 Weak Connectivity Model in Subsection

Consider an n -dimensional hypercube with a total of N sensor nodes, and each node in the network is assigned to a unique coordinate $j_1 j_2 \dots j_n$, where $0 \leq j_1, \dots, j_n < v$ and

$v = \lceil \sqrt[n]{N} \rceil$. For simplicity that n -dimensional hypercube can be expressed as $H(v, n)$. In addition, every valid coordinate can be divided into r subsections in sequence, each of which has no more than k characters, where $r = \lceil n/k \rceil$.

Definition 1. The nodes A and B in $H(v, n)$ are called logic neighbors, iff that only one character is different in their coordinates (as indicated in **Requirement1**). Both the two nodes are called physical neighbors, iff that they are within each other's signal range (as indicated in **Requirement2**, where d_r denotes node's signal range). There exists a secure link between A and B if they are neighboring both logically and physically.

$$\text{Requirement1: } d_h(A, B) = 1 \quad (1)$$

$$\text{Requirement2: } d_e(A, B) \leq d_r \quad (2)$$

Definition 2. The nodes A and B in $H(v, n)$ are called logic neighbors in subsection, iff that only one section has different characters in their coordinates.

Definition 3. For a given character string with the length of $n-k$, $b_1 b_2 \dots b_{n-k}$, the corresponding k -dimensional hypercube $H(k)$ contains v^k nodes and can be expressed as $b_1 b_2 \dots b_{n-k} * \dots *$, where $*$ denotes a character within $0, \dots, v-1$.

Definition 4. (k -dimensional weak-connectivity in subsection): The hypercube $H(v, n)$ is k -dimensional weak-connected in subsection, if the number of all reachable nodes in each section is larger than $v^k / 2$.

Lemma 1. Let an n -dimensional Hypercube $H(v, n)$ satisfies the conditions of k -dimensional weak-connectivity in subsection. Then all the reachable nodes form a connected graph in any two k -dimensional sub-hypercube neighboring in subsection.

Proof. Assume that $r = \lceil n/k \rceil$, a coordinate of the length n is then divided into r sub-strings with the length of no more than k . Let H_k and H'_k are two subsection neighboring k -dimensional sub-hypercubes, expressed as $H_1(k) = b_1 b_2 \dots b_{(r-1)k} \alpha_1 \dots \alpha_k b_{(r+1)k} \dots b_{n-k} * \dots *$ and $H_2(k) = b_1 b_2 \dots b_{(r-1)k} \beta_1 \dots \beta_k b_{(r+1)k} \dots b_{n-k} * \dots *$. Assume that the nodes u and v are reachable nodes, which belong to $H_1(k)$ and $H_2(k)$ respectively. Let $u = b_1 b_2 \dots \alpha_1 \dots \alpha_k \dots b_{n-k} x_1 x_2 \dots x_k$ and $v = b_1 b_2 \dots \beta_1 \dots \beta_k \dots b_{n-k} y_1 y_2 \dots y_k$. According to the property of k -dimensional weak-connectivity in subsection, there exist a reachable u_l node in $H_1(k)$ and a reachable v_l node in $H_2(k)$, expressed as $u_l = b_1 b_2 \dots \alpha_1 \dots \alpha_k \dots b_{n-k} c_1 c_2 \dots c_k$, and $v_l = b_1 b_2 \dots \beta_1 \dots \beta_k \dots b_{n-k} c_1 c_2 \dots c_k$. Note that the two nodes u_l and v_l are reachable and they both belong the sub-hypercube $H_c(k)$, denoted as $H_c(k) = b_1 b_2 \dots b_{(r-1)k} * \dots * b_{(r+1)k} \dots b_{n-k} c_1 \dots c_k$. As the sub-hypercube $H_c(k)$ satisfies the conditions of k -dimensional weak-connectivity in subsection, there exists a reachable node c , expressed as $c = b_1 b_2 \dots b_{(r-1)k} d_1 \dots d_k b_{(r+1)k} \dots b_{n-k} c_1 \dots c_k$. The nodes u_l , v_l and c are connected in $H_c(k)$. Thus the nodes u and v are connected.

Lemma 2. All of the reachable nodes in n -dimensional Hypercube $H(v,n)$, which satisfies the conditions of k -dimensional local-weak-connectivity in subsection, form a connected graph.

Proof. For simplicity, we express a valid coordinate of a node with the length of n as a string containing t characters. Assume that the nodes $u = a_1a_2...a_r$ and $v = b_1b_2...b_r$ where $a_i, b_i \in [0, kv-1]$. With regard to a subsection $a_i, b_i, i \in [0, r]$, there exists a subsection c_i , which enables the nodes u and u_i connected in $H_i(k)$ where $u_i = a_1...a_{i-1}c_i a_{i+1}...a_r$ and $H_i(k) = a_1 a_{i-1} * a_{i+1}...a_r$. Also it makes the nodes v and $v_i = b_1...b_{i-1}c_i b_{i+1}...b_r$ connected in $H_i(k) = b_1 b_{i-1} * b_{i+1}...b_r$. Thus along with no more than $2r-1$ intermediate nodes, such as $u_1, u_2...u_{r-1}, c = c_1 c_2...c_r, v_1, v_2...v_{r-1}$, the nodes u and v are connected.

3.2 Indirect Key Establishment

Assume that the two physically neighboring nodes A (i_1, i_2, \dots, i_n) and B (j_1, j_2, \dots, j_n) want to establish pairwise key between them. In case that $d_h((i_1, i_2, \dots, i_n), (j_1, j_2, \dots, j_n)) = k > 1$, the nodes perform the algorithm on indirect key establishment called **Inter-Area(S,D)** illustrated as follows.

The algorithm assumes that during the deployment phase nodes are required to exchange their connectivity information in subsection. That is, every node maintains a table T to record reachable nodes in each subsection. Let $S(a_1...a_n)$ and $D(b_1...b_n)$ be the two physically neighboring nodes. As the assumption of the algorithm has addressed, they exchange with each other their connection information in each subsection. Assume that the source node S initiates the key establishment phase. It thus creates a temporary table called T_D to record reachable nodes in common subsection code with those of node D . Node S then performs the following procedures:

P1: The subsection process on node's coordinate, such as $a_1...a_n \rightarrow a_1', a_2'...a_r', b_1...b_n \rightarrow b_1', b_2'...b_r'$ where $a'_j, b'_j \in [0, kv-1]$.

P2: Node S maintains a set of different subsections from the node D , denoted as $\ell = \{d_1, d_2, \dots, d_w\}_{d_1 < d_2 < \dots < d_w}$, and a path list P to recode the constructed key path.

P3: Node S checks T_D to find if there exist available nodes in each different subsection. If no available nodes in one of the subsections, the algorithm terminates. Otherwise it goes on the next procedure.

P4: Initialize the path $P: P \leftarrow S$ and the temporary node $C(c_1c_2...c_r): C = \leftarrow S$.

P5: FOR $(i=1; i \leq w; i++)\{$

IF $(c_i \neq b'_i) \{$

Search a reachable node in the i^{th} subsection: $C_i = c_1...c_{i-1}x_i c_{j+1}...c_r$ in the table T_D ;

Add the intermediate nodes along with the path between $C(c_1c_2...c_r)$ and $C_i(c_1...c_{i-1}x_i c_{j+1}...c_r)$ to P in sequence;

}

$C(c_1c_2...c_r): C = \leftarrow C_i$;

$P: P \leftarrow C$;

}

It's comparatively reasonable to model a sensor network in a small area as a hypercube with the properties of k -dimensional weak-connectivity in subsection. As one of necessary requirements, at least $(2^{k-1} + 1)^r$ nodes are to be reachable for a network containing 2^n nodes. Let us consider a network with $N=500$ and $k=r=3$. If the deployment area can be divided 8 sub-areas, each of which owns 8 groups, a reachable nodes is required to be connected at least 5 areas and 25 groups. As sensors are assumed densely distributed in a small area, we believe that such requirements can be satisfied normally.

4 A Clustering Scheme for Inter-area Key Path Establishment

In case of a sensor network deployed in a large deployment field with a huge number of sensors, it is not reasonable to apply the properties of k -dimensional weak-connectivity in subsection to construct a key path throughout the network. Fig.1a shows that there exist a large number of isolated connected graphs in a situation of $N=4000$. Even though some graphs may be overlapped physically, no key path available to connect them with each other. Furthermore, it should never be ignored that a fairly large number of isolated single nodes are available, as described in Fig.1b. In this section, we present a security protocol and a corresponding clustering algorithm, aiming at achieving further clustering by establishing a secure key path among those isolated graphs.

4.1 A Security Protocol for Pairwise Key Establishment

We denote those isolated connected graphs in Fig.1a as $G_1(V_1, E_1), G_2(V_2, E_2), \dots, G_k(V_k, E_k)$. We assume that nodes u and v are located in $G_1(V_1, E_1), G_2(V_2, E_2)$ respectively. That is, $u \in V_1$ and $v \in V_2$. We also assume that the two nodes are located within each other's signal range. Either of these two sensors are required to broadcast a request message with their IDs. Thus nodes u and v can know if logical neighboring nodes of the peers are available in its connected graph. Without loss of generality, we assume u has been sure that there exist a node in V_1 , u_m , is a logical neighboring node of v . The security protocol is presented as follows.

P1: $u \rightarrow u_1 \rightarrow u_2 \dots \rightarrow u_m : M$

Within a connected graph $G_1(V_1, E_1)$ node u can achieve a key path by performing the algorithm *Inter-Area(S,D)* addressed in Section3. A sequence of sensors u_1, u_2, \dots, u_m , that satisfy the requirements (1) and (2), form a key path for u to establish a pairwise key with node u_m .

Node u generates a random number r and initializes an arbitrary sequence number seq . It constructs a message $M = \{u, v, d, \{r, seq\}_{k_{temp}}\}$. Here d denotes the d^{th} different sub-index between nodes u_m and v , k_{temp} denotes currently used pairwise key, such as k_{u, u_1} for node u and its next hop u_1 . Consider node u_1 having the message

$M = \{u, v, d, \{r, seq\}_{k_{ump}}\}$. It decrypts the information and then encrypts it by using the pairwise key shared with its next hop such as u_2 . Similar procedures are performed by the following nodes until the message has been transmitted to the destination, u_m .

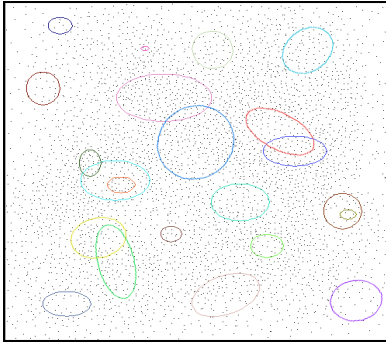


Fig. 1a. Isolated connected graphs are available in hypercube-based scheme

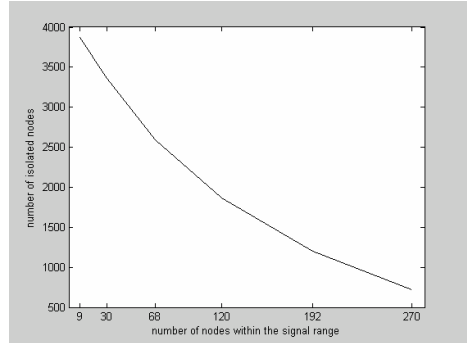


Fig. 1b. Relationship between number of isolated nodes and node distribution density given $N=4000$

P2: $u_m \rightarrow u : \{u, v, d, \{M'\}_{k_p}, \{r_1, ack\}_{k_u}, MAC\}$

When node u_m receives the message M , it performs the following processes. First, it calculates $k_u = F(r, seq)$ and encrypts $\{r_1, ack\}$. Here, F is a pseudo random function, r_1 is a random number generated by itself. The field ack is an acknowledgement corresponding to seq such that $ack = f(seq)$, for the received message. Then it chooses the specific polynomial share $f_{u_m}^d(u_m, v)$ to create the pairwise key between nodes u_m and v , expressed as $k_p = f_{u_m}^d(u_m, v)$. Notes that it is used for encryption on the message $M' = \{u, v, ack, r_1\}$. Finally it creates the message authentication code $MAC = C_{k_u}(u, v, d, \{M'\}_{k_p}, \{r_1, ack\}_{k_u})$ and forwards them to node u .

P3: $u \rightarrow v : \{u, v, d, \{M'\}_{k_p}\}$

After receiving the message, node u performs the following procedures.

Verification1: Confirm that $D_{k_u}(MAC) = h(u, v, d, \{M'\}_{k_p}, \{r_1, ack\}_{k_u})$

Verification2: Decrypt $\{r_1, ack\}_{k_u}$ to recover r_1 and ack . Confirm that $ack = f(syn)$.

Notes that node u also has ability to achieve the pairwise key $k_u = F(r, syn)$. By performing above verifications, it authenticates MAC to make sure that the reply, which aims at the specific message M , is actually originated by node u_m . It then forwards the message $\{u, v, d, \{M'\}_{k_p}\}$ to node v directly.

P4: $v \rightarrow u : \{ack, r_1\}_k$

After receiving the messages described above, node v first performs the consistency check based on established pairwise key by using the selected polynomial share

$f_v^d(v, y)$. It then calculates a session key $k'=F(r_l, c)$, where F is a pseudo random function. Finally, it generates a random number r_v and transmits the message $\{ack, r_v\}_{k'}$ back to node u .

P5: $u \rightarrow v : \{r_v\}_k$.

Once node u has received the message, it creates a session key $k'=F(r_l, c)$ as it has gained r_l from node u_m . Then it performs the following verification.

Verification3: Decrypt $\{ack, r_v\}_{k'}$ to recover r_v and ack . Confirm that $ack = f(syn)$.

If the verification is successful, it means that the sender is actually the node v . In addition, the reply from the node v is also validated as it responds properly for node u 's request.

Node v then performs the following verification to check if node u has sent back the correct r_v , which is used for pairwise key establishment.

Verification4: Confirm that $D_k(\{r_v\}_{k'}) = r_v$.

The procedure is illustrated as follows.

P1: $u \rightarrow u_1 \rightarrow u_2 \dots \rightarrow u_m : M$

P2: $u_m \rightarrow u : \{u, v, d, \{M'\}_{k_p}, \{r_l, ack\}_{k_u}, MAC\}$

P3: $u \rightarrow v : \{u, v, d, \{M'\}_{k_p}\}$

P4: $v \rightarrow u : \{ack, r_v\}_k$.

P5: $u \rightarrow v : \{r_v\}_k$.

4.2 Security Analysis

Our protocol can be divided into three phases: 1). Intermediate indirect key establishment phase. 2). Authorized information exchange phase. 3). Key path establishment phase. With regard to the first one, a secure key path is established, along with which any two adjacent nodes share a direct key. Thus, sensible information such as r is invisible to any other parties even though they do hear the communications.

The second phase is the heart of the protocol, as it concerns with authentication issue among three parties, such as node u , u_m and v . With regard to node u , **Verification1** and **Verification2** are necessary as it wants to make sure that the reply is actually originated by node u_m . On the other hand, node u_m generates r_l , which enables the other two nodes to create a session key individually. In addition, node u_m uses k_u and k_p to encrypt messages separately, thus achieving node authentication during message exchange. Notes that k_u and k_p are only expected to be created by the designated parties.

The focus of the third phase is the authentication issue on communications between nodes u and v . Notes that node v receives a message with no attachments, it has to initiate a challenge, r_v to the peer node as well as to send back a proper ack . By performing **Verification3**, node u has a proof to confirm node v 's identification. In addition, based on **Verification4**, node v is sure that there exists trust relationship

between nodes u and u_m . Any other node would fail to response the challenge successfully as it has no means to achieve k' .

Also, mechanisms such as fault tolerance have been taken into serious consideration. In order to prevent message exchange from network failures, sequence number is introduced to identify a specific round of key path establishment. Any other replies would be discarded if the containing *ack* does not corresponding to a current *seq*.

4.3 A Clustering Algorithm on Inter-area Key Path Establishment

Consider the two nodes u and v such that $u \in V_1, v \in V_2$, and $d_e(u,v) \leq d_r$. Obviously, $d_h(u,v) = k > 1$ is held. Based on the contributions of exchange protocol described in Section 4.1, those two nodes that satisfy the following requirements can establish pairwise key.

Requirement3: $\exists w_1 \in G_1, d_h(w_1, v) = 1$ or

$$\exists w_2 \in G_2, d_h(u, w_2) = 1 \tag{3}$$

Thus, those isolated graphs can be clustered further by means of the following algorithm, for purpose of achieving global connectivity through the entire network.

Graph Clustering Algorithm (G_1, G_2, \dots, G_k)

- P1: Initialize temporary variables and data structures.
- P2: For ($i=1; i \leq k; i++$)
 - {
 - If G_i has never been clustered {
 - $j=j+1$;
 - $G_j' = G_i$;
 - For ($l=i+1; l \leq k; l++$)
 - {
 - if (**Requirement3** can be satisfied)
 - $G_j' = G_j' \cup G_l$;
 - }
 - }
- P3: Output a set of clustered graphs G_1', G_2', \dots, G_k' .

5 Performance

Average number of hops of a key path in inner-area scheme

Consider two nodes $u = a_1 a_2 \dots a_r$ and $v = b_1 b_2 \dots b_r$ where $a_i, b_i \in [0, kv - 1]$. The probability of $a_i = b_i$ for any $i \in \{1, \dots, r\}$ is $1/kv$, and the probability of having exactly i different subsection is

$$p[i] = \frac{r!}{i!(r-i)!} \cdot \frac{1}{(kv)^{r-i}} \cdot \left(1 - \frac{1}{kv}\right)^i.$$

Thus, the average key path length ignoring the factor of signal range can be estimated by $L_l = \sum_{i=1}^r (2i-1)p[i]$. As the scheme has addressed, we only concern about $v^k/2$ connected nodes in each subsection. In the worst situation, those nodes may be connected with each other one by one within the signal range, thus the approximate average number of hops is about $v^k/4+1$. Then the average number of hops in a key path can be expressed as $L_h = (\frac{v^k}{4} + 1) \cdot \sum_{i=1}^r (2i-1)p[i]$.

Figure 2 shows the relationship between the average number of hops and the number of subsections given different local network sizes. The number of hops drops dramatically as the number of subsections grows. Also we can see the larger the network is, the more the required hops.

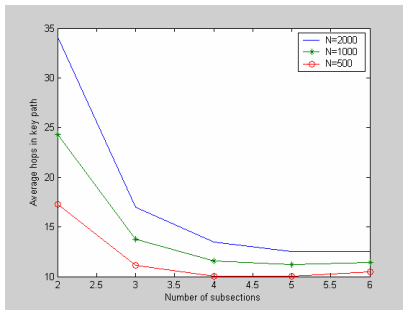


Fig. 2. Average number of hops of a key path in inner-area scheme

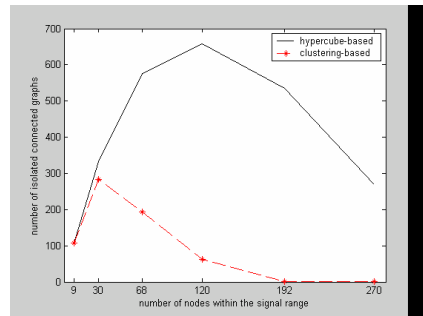


Fig. 3. Relationship between number of isolated connected graphs and node distribution density

Probability to achieve graph clustering

Consider two sensors $u (u_1u_2...u_n)$ and $v(v_1v_2...v_n)$ where $u \in G_i$ and $v \in G_j$. The probability of having only one different sub-index is $p_1 = n(m-1)/m^n$. Assume that there are N_i and N_j sensors in each area. For a given node u (or v), the probability of having at least one different sub-index in G_j (or G_i) can be expressed as $p_l = (1 - P_{N_i-1}^0) + (1 - P_{N_j-1}^0) - (1 - P_{N_i-1}^0) \cdot (1 - P_{N_j-1}^0) = 1 - P_{N_i-1}^0 \cdot P_{N_j-1}^0 = 1 - (1 - p_1)^{N_i + N_j - 2}$

Fig. 3 shows relationship between number of isolated connected graphs and node distribution density given $N=4000$. In case of a network with sparsely distributed nodes, the number of connected graphs is fairly small, as there exist a huge number of “single” nodes. Isolated connected graphs grow dramatically before the node distribution density gets to a certain point. Then number of connected graphs drops as more and more nodes are covered within the signal range. Compared with hypercube-based scheme, our clustering scheme produces much less isolated graphs, converges more quickly on graph clustering, and thus achieves higher probability on global connectivity establishment.

6 Conclusion

Due to energy constraints and random distribution of nodes in sensor networks, we argue that it has some limitations to model connectivity of nodes as a pure hypercube for analysis. We have made two approaches to achieve pairwise key path establishment according to different network sizes. Firstly, we consider a simple situation such as a local network with densely distributed nodes. It is more reasonable to model such a network as a hypercube, and we inspect the connectivity issue in subsection to deal with the situation of a number of nodes are out of communication. Secondly, aiming at the clustering issue on isolated connected graphs in a large target field, we present a security protocol for key path establishment in inter-area communications. Based on the contributions of our protocol, the resulting schemes have nice performance on probability to establish pairwise key through the entire network.

References

1. Chong, C.-Y., Srikanta, P.K.: Sensor Networks: Evolution, Opportunities, And Challenges. *Proceeding Of The Ieee* 91(8), 1247–1256 (2003)
2. Du, W., Deng, J., Han, Y.S., Et Al.: A Pairwise Key Predistribution Scheme For Wireless Sensor Networks. In: *Proceedings Of 10th Acm Conference On Computer And Communication Security*, pp. 42–51 (2003)
3. Estrin, D., Govindan, R., Heideman, J., Kumar, S.: Next Century Challenges: Scalable Coordination In Sensor Networks. In: *Proceedings Of The 5th Annual Acm/Ieee International Conference On Mobile Computing And Networking*, pp. 263–270 (1999)
4. Eeschnaure, I., Gligor, V.D.: A Key-Management Scheme For Distributed Sensor Networks. In: *Proceedings Of The 9th Acm Conference On Computer And Communication Security*, pp. 41–47 (2002)
5. Blundo, C., Desantis, A., Kuten, S., Et Al.: Perfectly Secure Key Distribution For Dynamic Conferences. In: Brickell, E.F. (Ed.) *Crypto 1992. Lncs, Vol. 740*, pp. 471–486. Springer, Heidelberg (1993)
6. Chan, H., Oerrig, A., Song, D.: Random Key Predistribution Schemes For Sensor Networks. In: *Ieee Symposium On Research In Security And Privacy*, pp. 197–213 (2003)
7. Liu, D., Ning, P., Li, R.: Establishing Pairwise Keys In Distributed Sensor Networks. *Acm Transactions On Information And System Security* 8(1), 41–77 (2005)
8. Liu, D., Ning, P.: Location-Based Pairwise Key Establishments For Static Sensor Networks, Available From [Http://Discovery.Csc.Ncsu.Edu/Pning/Pubs/Sasn03.Pdf](http://Discovery.Csc.Ncsu.Edu/Pning/Pubs/Sasn03.Pdf)

An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks

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. RFID technology is a ubiquitous technology, and seems destined to become more and more ubiquitous. Traditional cryptographic primitives are not supported on low-cost RFID tags since, at most, 4K gates can be devoted to security-related tasks. Despite this, there are a vast number of proposals based on the use of classical hash functions, an assumption that is not realistic (at least at the present time). Furthermore, none of the published authentication protocols are resistant to active attacks. We try to address these two issues in this work by designing a new authentication protocol, secure against passive and active attacks, inspired by Shieh et al.'s protocol for smart-cards, but adapted to RFID systems. The original Shieh et al.'s scheme is considered one of the most secure and efficient protocols in the smart-card field. Because in this protocol tags should support a hash-function on-board, a new lightweight hash function, named *Tav-128*, is also proposed. A preliminary security analysis is shown, as well as a study on its hardware complexity, which concludes that its implementation is possible with around 2.6K gates.

Keywords: IUC, RFID, Security, Active-attacks, Authentication, Lightweight Hash functions.

1 Introduction

One of the main problems that ubiquitous computing has to solve before its wide development is privacy [1]. In the RFID context, products labeled with insecure tags reveal sensitive information when queried by readers. Additionally, tags usually answer different queries with the same identifier. These predictable tag responses allow a third party to establish an association between tags and their owners. In addition to the previous threats, there are some other aspects that must be considered: eavesdropping, counterfeiting, physical attacks, active attacks, etc. To depth in all these matters we recommend the reading of [2,3,4] where surveys of the most important advances in RFID technology are presented.

Low-cost RFID tags are very computationally limited devices due to its severe price restriction (.05 - 0.1 €). Tags can only store hundreds of bits, and have 250-4K gates to implement security functions [5]. Even under these conditions, most of the proposed solutions in the literature are based on hash functions or

PRNGs [6,7,8,9]. From a theoretical point of view, these proposals have helped to increment the security level of RFID systems. However, none of these proposals are realistic. Note that for implementing traditional hash functions significantly more resources are needed. On the other hand, lightweight protocols can be fitted in low-cost RFID tags, because they only perform very simple operations. Nevertheless, none of the existing proposals are resistant to active attacks. In most of the cases, these kind of attacks are simply discarded as not applicable, which may be false in some real-life scenarios. Recently, Cui et al. have proposed the use of asymmetric cryptography to solve active attacks [10]. However, nowadays the usage of asymmetric cryptography, although being an active research field [11,12] is not considered to be possible in low-cost RFID tags.

The kind of attacks applicable to RFID technologies are not much different to those that can happen in wireless, bluetooth, or smart-card systems. We have found interesting resemblances in the field of smart-card security, which is by now a consolidated technology. Since the pioneer work of Lamport (1981) where he proposed a remote authentication scheme, many researchers suggested alternative schemes improving the efficiency and security of remote authentication processes. Recently, Shieh et al. have proposed a very interesting scheme in their work entitled “Efficient remote mutual authentication and key agreement” [13]. This protocol is considered to be one of the most secure and efficient security protocols for smart-cards. Taking advantage of this work, we have updated their protocol to the characteristics of RFID systems. The resulting protocol is not only resistant to the standard passive attacks, such as privacy, tracking and eavesdropping, etc. but also to active attacks. As the protocol is based on the use of hash functions, we have also designed a new lightweight hash function, named *Tav-128*. A security and performance analysis of this new function is presented, showing its applicability to low-cost RFID tags.

The rest of the paper is organized as follows. In *Sect. 2*, Shieh et al.’s protocol is described. *Sect. 3* proposes a new protocol inspired in Shieh et al.’s scheme but adapted to RFID systems. A security analysis is presented in *Sect. 4*. A new lightweight hash function is proposed in *Sect. 5*, including a preliminary security and performance analysis. Finally, we draw some conclusions in *Sect. 6*.

2 Review of Shieh et al.’s Scheme

The security of Shieh et al.’s scheme (2006) is based on the use of secure one-way hash functions (Merkle, 1989; NIST FIPS PUB 180, 1993; Rivest, 1992). Time stamps are used but no time-synchronization is required. The scheme consists in two phases: the registration phase, and the login and key agreement phase.

2.1 Registration Phase

Assume an user U_i submits his identity ID_i and password PW_i to the server over a secure channel for registration. If the request is accepted, the server computes

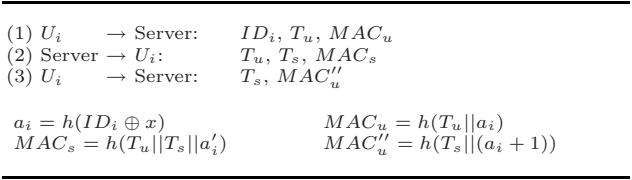


Fig. 1. Messages transmitted in Shieh’s scheme

$R_i = h(ID_i \oplus x) \oplus PW_i$ and issues U_i a smart-card containing R_i and $h()$, where $h()$ is a one-way hash-function, x is the secret key maintained by the server, and the symbol “ \oplus ” denotes the exclusive-or operation.

2.2 Login and Key Agreement Phase

Fig. 1 is an illustration of messages transmitted during the login and key agreement phase in Shieh’s scheme. When user U_i wants to login to the server, he first inserts his smart-card into a card reader then inputs his identity ID_i and password PW_i . Next, the smart-card performs the followings steps:

1. Compute $a_i = R_i \oplus PW_i$.
2. Acquire current time stamp T_u , store T_u until the end of the session, and compute $MAC_u = h(T_u || a_i)$.
3. Send message (ID_i, T_u, MAC_u) to the server.

After receiving message (ID_i, T_u, MAC_u) from U_i , the server performs the following steps to assure the integrity of the message, answer to U_i , and challenge U_i to avoid replay attacks:

1. Check the freshness of T_u . If T_u has already appeared in a current execution session of user U_i , reject U_i ’s login request and stop the session. Otherwise T_u is fresh.
2. Compute $a'_i = h(ID_i \oplus x)$, $MAC'_u = h(T_u || a'_i)$ and check whether MAC'_u is equal to the received MAC_u . If it is not, reject U_i ’s login and stop the session.
3. Acquire current time stamp T_s . Store temporarily paired time stamps (T_u, T_s) and ID_i for freshness checking until the end of the session. Compute $MAC_s = h(T_u || T_s || a'_i)$ and session key $K_s = h((T_u || T_s) \oplus a'_i)$. Then, send the message (T_u, T_s, MAC_s) back to U_i .

On receiving the message (T_u, T_s, MAC_s) from the server, the smart-card performs the following steps to authenticate the server, achieves a session key agreement, and answers to the server.

1. Check if the received T_u is equal to the stored T_u to assure the freshness of the received message. If is not, report login failure to the user and stop the session.

2. Compute $MAC'_s = h(T_u || T_s || a_i)$ and check whether it is equal to the received MAC_s . If not, report login failure to the user and stop. Otherwise conclude that the responding party is the real server.
3. Compute $MAC''_u = h(T_s || a_i + 1)$ and session key $K_s = h((T_u || T_s) \oplus a_i)$, then send the message (T_s, MAC''_u) back to the server.

When the message (T_s, MAC''_u) from U_i is received, the server performs the following steps to authenticate U_i and achieve key agreement:

1. Check if the received T_s is equal to the stored T_s . If it fails reject U'_i login request and stop the session.
2. Compute $MAC'''_u = h(T_s || (a'_i + 1))$ and check whether this is equal to MAC''_u . If it is not, reject U_i 's login request and stop the session. Otherwise, U_i is a legal user and U_i 's login is permitted. At this moment, mutual authentication and session key agreement between U_i and the server are achieved.

3 Our Scheme

In this section, a new protocol adapted to RFID systems and resistant to passive and active attacks (inspired in Shieh et al.'s protocol) is proposed. First, we will mention some peculiarities of RFID systems which should be considered in the new design. These will force changes in the protocol, which will be presented next.

In Shieh et al.'s protocol, when the user wants to login in the server "*he first inserts the card into a card-reader...*". In a RFID system, tags (T) will be equivalent to smart-cards and readers to card-readers, respectively. Note RFID readers (R) are assumed to be connected to back-end databases (B) over a secure channel. Additionally, both devices have "non-limited" computing and storing capabilities. In the following, when we refer to a RFID reader an entity composed by a reader and a back-end database is considered.

However, there are significant differences between smart-card and RFID systems. RFID technology operates through the radio channel, so communication could be eavesdropped. Another particularity is the asymmetry of the communication channel, which allows monitorization of the forward channel (reader-to-tag) from a much longer distance than the backward channel (tag-to-reader). Smart-cards are usually tamper resistant devices, which is not the case of RFID tags. Furthermore, when then smart-card is inserted in the reader an user intervention is necessary, entering his identity and password. In RFID technology, however, interactions between tags and readers are automatic.

Taking into account all these considerations, Shieh et al's scheme has been adapted. Our proposed scheme consists on two phases: the registration phase, and the mutual authentication and index-pseudonym update phase. The following symbols have been used:

- | | |
|---|--------------------------------------|
| x_i : secret key maintained by the reader | N_z : random number generated by z |
| $h()$: secure one-way hash function | \oplus : exclusive-or operation |
| $ $: string concatenation operation | |

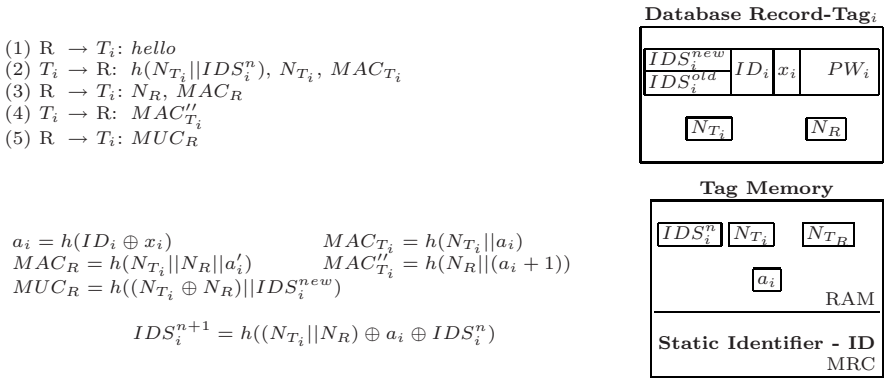


Fig. 2. Messages transmitted in our protocol

3.1 Registration Phase

The user or holder of the tag submits his static identifier ID_i and a freely chosen password PW_i to the reader over a secure channel for registration. If the request is accepted, the reader generates a random index-pseudonym IDS_i^0 and computes $a_i = h(ID_i \oplus x_i)$.¹ The tag will replace its identifier ID_i by IDS_i^0 and store a_i . The IDS_i^n will be used as searching-index of a database in which all the sensitive information (ID_i , x_i , PW_i) and the temporary data session (N_{T_i} , N_R) associated with each tag are stored. IDS_i^{new} and IDS_i^{old} are initially set to IDS_i^0 . The password PW_i will be used by the holder of the tag (over a secure channel) to temporarily deactivate the tag. In this case, a_i will be replaced by $R_i = a_i \oplus PW_i$.

3.2 Mutual Authentication and Index-Pseudonym Update

The messages interchanged in our scheme are shown in *Fig. 2*. First, the reader usually applies a probabilistic (ie. Aloha-based algorithm) or determinist (ie. Binary tree-walking protocol) collision avoidance protocol to singulate a tag out of many tags. Upon singulation condition, the reader will send a “hello” message to the tag. To start the mutual authentication, the tag accomplishes the following steps:

1. Generate a random number N_{T_i} , and store N_{T_i} temporarily until the end of the session.

¹ A 64-bit length identifier is compatible with all the encoding schemes (SGTIN, SSCC, GLN, etc) defined by EPCGlobal. Due to this reason, we assume that tag static identifier (ID_i), and index-pseudonyms (IDS_i^n) are 64-bit length. Additionally, the secret key x_i is xored with ID_i to compute a_i , so x_i length is also set to 64-bits.

² Tags conforming with EPC Class-1 Gen-2 specification support a 16-bit PRNG. We suggest that 32-bit PRNGs should be supported on low-cost RFID tags, as mentioned in. So, 32-bit length could be an adequate value to N_{T_i} and N_R .

2. Compute $h(N_{T_i}||IDS_i^n)$, and $MAC_{T_i} = h(N_{T_i}||a_i)$.
3. Send message $(h(N_{T_i}||IDS_i^n), N_{T_i}, MAC_{T_i})$ to the reader and wait for response.

Once the previous message is received, its integrity is checked and the reader answer includes a challenge to avoid replay attacks:

1. Check the newness of N_{T_i} . If N_{T_i} has already come out in a current mutual authentication, the protocol is stopped in this point. Otherwise N_{T_i} is fresh.
2. Compute $p' = h(N_{T_i}||IDS_i^{new})$ and $p'' = h(N_{T_i}||IDS_i^{old})$ and check whether any of the two values is equal to the received $h(N_{T_i}||IDS_i^n)$. The above procedure is repeated for each entry (row) in the database until a match is found. If not found, the protocol is stopped at this point.
3. Compute $a'_i = h(ID_i \oplus x_i)$, $MAC'_{T_i} = h(N_{T_i}||a'_i)$, and check if it is equal to MAC_{T_i} . If not, the protocol is stopped and a check over tag deactivation is taken by computing $R'_i = a'_i \oplus PW_i$, $MAC'_{T_i} = h(N_{T_i}||R'_i)$ and verifying if it is equal to MAC_{T_i} . A match will imply that the tag has been deactivated temporally by its holder.
4. Acquire a fresh random number N_R .² For avoiding replay attacks, the pair (N_{T_i}, N_R) is stored until the end of the session.
5. Compute $MAC_R = h(N_{T_i}||N_R||a'_i)$. Then, send the message (N_R, MAC_R) back to the tag and wait for response.


After receiving the message (N_R, MAC_R) , the following steps are accomplished to authenticate the reader, achieve new material to update the index-pseudonym, and finally answer to the reader:

1. Compute $MAC'_R = h(N_{T_i}||N_R||a_i)$ and check if its value is equal to the received MAC_R . If not, stop the protocol at this point. Note that the newness of this message is guaranteed by N_{T_i} . For preventing loss of synchronization attacks, N_R is also stored in the tag.
2. Compute $MAC''_{T_i} = h(N_R||a_i + 1)$ and send it back to the reader.

When the message MAC''_{T_i} is received, the reader computes $MAC'''_{T_i} = h(N_R||a'_i + 1)$ and checks whether it is equal to MAC''_{T_i} . If not, the protocol is stopped. At this point, both the reader and the tag have mutually authenticated. Additionally, both possess two nonces (N_{T_i}, N_R) , which have been interchanged. Shieh et al. proposed using this fresh material to establish a session key agreement. In our case this material is employed to update the index-pseudonym. Obviously, the tag and reader have to be synchronized.

The glib solution for the synchronization problem will be to update the index-pseudonym in the tag when message 4 is sent, and this updating will be performed in the reader when checking this message. Under this scenario an attacker (active attack) could intercept message 4 avoiding the update of the index-pseudonym in the reader with the consequently losing of synchronization. A naive solution will consist on assuming that after the end of the protocol, completion messages are sent between the involved entities. However, these messages

could be also intercepted. Additionally, note that tags are much more constrained devices than readers. For this reason, a new message 5 has been added to the protocol (Message Update Code - MUC), and readers will have to store the old and the new index-pseudonym to prevent the interception of this message. To complete the protocol, the following steps are performed by the reader:

1. Store the current session index-pseudonym $IDS_i^{old} = IDS_i^{new}$ to avoid desynchronization attacks.
2. Compute the new index-pseudonym $IDS_i^{new'} = h((N_{T_i} || N_R) \oplus a'_i \oplus IDS_i^{new})$ 
3. Compute $MUC_R = h((N_{T_i} \oplus N_R) || IDS_i^{new'})$ and send it to the tag, including the two nonces interchanged between reader and tag and the new index-pseudonym.

When the message MUC_R is received from reader, the tag accomplishes the following steps to verify a successfully index-pseudonym update has been performed in the reader:

1. Compute the potential-new index-pseudonym $IDS_i^{n+1} = h((N_{T_i} || N_R) \oplus a_i \oplus IDS_i^n)$.³
2. Compute $MUC''_R = h((N_{T_i} \oplus N_R) || IDS_i^{n+1})$ and check whether MUC''_R is equal to MUC_R . If this is the case, update the index-pseudonym.

4 Security Analysis

The robustness of the proposed protocol against the main important attacks is analyzed in the following.

1. User Privacy

Tag ID_i must be kept secure to guarantee user's privacy. In order to protect it, both the tag's memory and the radio channel have been taken into account. In the registration phase, the static identifier ID_i and the password PW_i are submitted to the reader over a secure channel. To avoid radio access to the static identifier, ID_i is replaced by the hash of $ID_i \oplus x_i$. Note, x_i is a secret key only known by the reader. Additionally, and similarly to what happens in e-passports, we recommended the ID_i to be printed as a machine-readable code as illustrated in *Fig. 2*. In the radio channel, the value of IDS_i^n is protected by the use of a secure one-way hash function $h(\cdot)$. In the same way, a_i can not be derived from the messages authentication codes MAC_{T_i} , MAC_R and MAC''_{T_i} .

2. Location Privacy

The secure protection of tag information does not ensure location privacy. Constant answers would allow an attacker to identify each tag with its

³ If tags support on board the proposed *Tav-128* hash function, a_i 's length will be fixed to 128-bits ($a_i = h(ID_i \oplus x_i)$). In this case, we suggest the following update equation: $IDS_i^{new'} = h((N_{T_i} || N_R) \oplus a'_i[0:63] \oplus a'_i[64:127] \oplus IDS_i^{new})$.

holder. To protect the index-pseudonym, only its hash is transmitted. As the index-pseudonym is not updated until the completion of the protocol, and the protocol may be accidentally or intentionally interrupted, the hash of the IDS_i concatenated with nonce N_{T_i} is really sent. Similarly, a_i is anonymized by means of the use of message authentication codes where a kind of challenge-response nonces are included. Finally, sending the message update code $MUC_R = h((N_{T_i} \oplus N_R) || IDS^{n+1})$, the new index-pseudonym is hidden. So, in order to avoid tracking, all the information is anonymized.

3. Data Integrity

Based on the use of a mutual authentication approach, our protocol guarantees data integrity between tag and reader. On the other hand, tag's memory is rewritable so modifications are possible. In this memory, both a_i and the index-pseudonym IDS_i^n are stored. If an attacker does succeed in modifying this part of the memory, the reader would not recognize the tag, having to carry out the registration phased again (see *Sect. 3.1*).

4. Mutual Authentication

Due to the fact that both tag and reader authenticate each other, by means of message authentication codes MAC_R and MAC''_{T_i} , mutual authentication is accomplished. These message authentication codes include a_i , a secret only shared between them, preventing any other to create correct MAC s, and in this way guaranteeing the legitimacy of each part. Therefore, it is infeasible for a fraudulent reader or tag to impersonate another entity.

5. Replay Attack

Our protocol is based on a challenge-response scheme, so replay attacks are prevented because challenges are different each time and long enough to prevent attacks based on storing them. In our scheme, any replay attack will not be able to correctly answer the challenges that form part of the protocol. In message 2, tag sends $(h(N_{T_i} || IDS_i^n), N_{T_i}, MAC_{T_i})$ where a nonce N_{T_i} is included. Therefore, the reader must include N_{T_i} in the answer message, so in message 3 the reader sends $(N_R, MAC_R = h(N_{T_i} || N_R || a'_i))$, including not only the response nonce N_{T_i} but also a challenge nonce N_R . Then, tag sends $MAC''_{T_i} = h(N_R || (a_i + 1))$ back, including N_R , to the reader. So, only legitimate parties (reader+tag) can send valid answers as challenge nonces are joined with the message authentication codes requiring the knowledge of a_i .

6. Forgery Resistance

All the sensitive information stored in the tag (IDS_i^n, a_i) is never sent in clear in the communication channel. In all cases, this information is concatenated with a nonce and hashed before passed on the channel. Therefore, the simple copy of information by eavesdropping is not useful to an adversary.

7. Active Attacks

(a) Man-in-the-middle attack: If an attacker tries to impersonate a legitimate reader to obtain information from a tag, perhaps to be able to impersonate it in a future. This kind of attack is not feasible because all messages include a message authentication code, which requires the knowledge of the secret a_i shared only between the tag and the reader. In

- the previous scenario, the fraudulent reader will not be able to generate message 3, so the capture of the message 4 sent back by the tag will be a vain attempt. Moreover, in future sessions, a new challenge would be used by the reader preventing any advantage from knowing old messages.
- (b) Parallel session: Because of the asymmetric structure of the message authentication codes $MAC_{T_i} = h(N_{T_i} || a_i)$ and $MAC''_{T_i} = h(N_R || a_i + 1)$ this attack fails. Another important point is that both reader and tag store the session nonces, N_{T_i} and N_R .
 - (c) Synchronization loss: The tag updates the index-pseudonym only when the message update code (MUC) is received. An attacker could interrupt this message, trying to de-synchronize reader and tag. To avoid this sort of attack, each time the reader updates the index-pseudonym, the old index-pseudonym is still maintained. Under the interception of the MUC from the reader, the tag will use the old index-pseudonym to build $h(IDS_i^n || N_{T_i})$. When the reader checks its integrity, it first will try with the new index-pseudonym, and if it fails, then he will try with the old index-pseudonym. Next, the rest of the protocol will be accomplished ensuring the recovery of a synchronization loss.

5 Hash-Function

Traditional cryptographic primitives exceed the capabilities of low-cost RFID tags. The required hardware complexity of these devices may be weighted up by its circuit area or the number of equivalent logic gates. At most, around 4K gates are assumed to be devoted to security-related task [5]. The best implementation of SHA-256 requires around 11K gates and 1120 clock cycles to performing a hash calculation on a 512-bit data block [18]. As the number of needed resources are quite higher than those of a low-cost RFID tag, it may seem natural to propose the use of another smaller hash functions. However, functions such as SHA-1 (8.1K gates, 1228 clock cycles) or MD5 (8.4K gates, 612 clock cycles) can not be fitted either in a tag [18]. Recently, some authors suggest the usage of a “universal hash function” [19]. Although this solution only needs around 1.7K gates, a deeper security analysis is needed and has not yet been accomplished. Furthermore, this function has only a 64-bit output, which does not guarantee an appropriate security level because finding collisions is a relatively easy task due to the birthday paradox (around 2^{32} operations). For this reason, we propose a 128-bit hash function named *Tav-128* that can be fitted in low-cost RFID tags and provides a suitable security level for most applications.

5.1 *Tav-128* Security Analysis

Some of the recent cryptanalytic attacks on many of the most important hash functions [20,21] rely in the fact that these constructions generally use a very linear (LFSR-based) expansion algorithm. In order to avoid this, we have decided to make the expansion of the *Tav-128* hash function (corresponding to algorithms C and D in the code shown in the *Appendix A*) highly nonlinear. As, on the

other hand, the resulting function should be very efficient and lightweight both from the gate count and the throughput point of view, we have found these functions by evolving compositions of extremely light operands by means of genetic programming, as described in [22].

We have also tried to include a filter phase (corresponding to algorithms A and B in the *Appendix A*) in the input of the *Tav-128* function, in order to avoid the attacker to have direct access to any bit of the internal state. Not having this possibility, some attacks that have been found on other cryptographic primitives in the past are precluded. So, decreasing the control the attacker has over the hash functions inputs significantly complicates his task.

An output length of 128 bits was found to be a reasonable compromise between speed and robustness to realistic attacks in the intended scenarios. Additionally, we propose the use of eight rounds in the internal loop (*r2* parameter) for having and adequate security margin, though we have found that even with six rounds (which will significantly improve its performance) the overall scheme seems to be secure.

We have performed an additional security analysis of *Tav-128*, consisting on examining the statistical properties of its output over a very low entropy input. Specifically, 2^{25} 32-bit inputs have been generated by means of an incremental counter (x , $x+1$, $x+2$, etc). After randomly initializing (with values obtained from <http://randomnumber.org>) the internal state and the accumulated hash $a0$ value, we compute the output of *Tav-128* for each counter value input ($Tav(x)$, $Tav(x+1)$, $Tav(x+2)$, etc). The resulting hashes have been analyzed with two well-known suites of randomness tests, namely ENT [23] and DIEHARD [24]. The results are presented in *Tables 1* and *2* (see *Appendix A*). *Tav-128* also passed the very demanding -because it is oriented to cryptographic applications- NIST [25] statistical battery. We have computed 100 p-values for each test, being all the results compatible with a uniform $U(0, 1)$. The whole report is available in <http://163.117.149.137/tav/> due to the huge amount of p-values generated.

Authors acknowledge that successfully passing these statistical batteries, even over a very low-entropy input, does not prove security, but we believe that it points out the nonexistence of trivial weaknesses.

5.2 Hardware Complexity

One of the most relevant aspects considered in the design of *Tav-128* was the sort of operations that can be employed. As tags are very restricted computationally, only simple operations have been used. For example, multiplication has been ruled out due to its high cost [26]. Concretely, the following operators have been finally used: right shifts, bitwise xor, and addition mod 2^{32} . The necessary architecture to implement *Tav-128* can be divided in two main blocks:

- **Memory blocks.** All the used variables are stored in this part: state (128-bits), accumulated hash $a0$ (32-bits), internal variables $h0$ (32-bits) and $h1$ (32-bits), and the input $a1$ (32-bits).
- **Arithmetic logic Unit.** In this unit the addition mod 2^{32} and the bitwise xor operation are implemented. As the $h0$ and $h1$ functions consist of three

or more components, an auxiliary register to store the intermediate results is necessary.

Although we have not implemented *Tav-128* in hardware, an overestimation of its gate counting can be easily obtained. The function bitwise xor requires 32 logic gates as we are operating with 32-bit variables. For implementing the add with carry circuit, a parallel architecture is proposed. Six logic gates are needed for each bit added in parallel⁴. The registers will be implemented by means of flip-flops. A gate count of 8 has been chosen for implementing a flip-flop as in [27]. So, 2304 logic gates are necessary to store the memory block and the auxiliary register. Additionally, around 50 extra logic gates are employed to control the internal state of the hash function. Therefore, 2578 logic gates are needed for implementing *Tav-128*.

Another key aspect to consider is throughput. We reckon that 1568 clock cycles are needed for executing one *Tav-128* hash. Due to the fact that low-cost RFID tags imply serious powers restrictions, we assume that the clock frequency is set to 100 KHz. Under this conditions, the throughput obtained by a tag that would have on-chip *Tav-128* will be around 65 hashes/sec. It is generally accepted that at least between 50-100 tags should be authenticated per second [28]. In other words, a tag may use up at the most 2000 clock cycles (@100Khz) to answer a reader. In some applications 65 hashes/sec may not be enough, so we have analyzed how to increment the speed of *Tav-128*. In the initial proposed scheme (see *Appendix A*), we have a parameter (r_2), which fits the number of rounds computed in the *C* and *D* algorithms. This parameter has been initially fixed to eight rounds in order to guarantee a high avalanche effect. After accomplishing a deeper study, we have determined that r_2 may be reduced to six rounds. So, the speed of the tag will be incremented in a 25% or in other words, the tag may compute around 80 hashes/sec. Note that for non-high speed demanding applications, we recommend to fix r_2 to eight rounds.

6 Conclusions

Since 2002, there has been a great number of publications concerned with the security of RFID technology. In the majority of those proposals, the security objectives are focused on privacy, tracking, counterfeiting, etc. All this kind of attacks are passive, but active attacks can not be ruled out in many scenarios.

A new protocol not only resistant to standard passive attacks but also resistant to active attacks is proposed. Another interesting property is that tags can be temporally deactivated without data loss. Instead of beginning from scratch, we have tried to avoid past errors in the designing of our protocol. RFID technology has similarities with other technologies such as wireless, bluetooth, smart-card, etc. Indeed, we focused our attention to smart-card, which is a mature technology. Concretely, we spotlight on remote authentication protocols, which started to be developed in 1980. During years many researchers have been working in

⁴ $S = A \oplus [B \oplus C_{ENT}] \quad C_{SAL} = B_{CENT} + A_{CENT} + AB.$

order to propose more secure and efficient schemes. Recently, Shieh et al. have proposed a new scheme that can be considered one of the most secure and efficient protocols. For this reason we decide to propose a new protocol for RFID systems inspired in Shieh et al.'s protocol.

The proposed protocol is based on the use of a secure hash function. As traditional cryptographic primitives such as SHA-256 or MD5 lie well beyond the capabilities of low-cost RFID tags, a new hash function (*Tav-128*) is proposed. *Tav-128* can be implemented with only around 2.6K gates, and 1568 cycles (1248 if *r2* parameter is set to six). Therefore, *Tav-128* can be fitted in a real low-cost RFID tags. Although further security analysis of the new hash function is needed, this preliminary analysis seems to point out that it gives an adequate security level for the intending application (mutual authentication of low-cost tags). To conclude, although this hash function constitutes a great advance, as a future work we plan to design a new version where the number of processing cycles was reduced without incrementing the number of logical gates.

References

1. Weiser, M.: The computer for the 21st century. *Scientific American* 265(3), 94–104 (1991)
2. Juels, A.: RFID security and privacy: A research survey. Manuscript (2005)
3. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J., Ribagorda, A.: RFID systems: A survey on security threats and proposed solutions. In: Cuenca, P., Orozco-Barbosa, L. (eds.) PWC 2006. LNCS, vol. 4217, pp. 159–170. Springer, Heidelberg (2006)
4. Piramuthu, S.: Protocols for RFID tag/reader authentication. *Decision Support Systems* 43, 897–914 (2007)
5. Ranasinghe, D., Engels, D., Cole, P.: Low-cost RFID systems: Confronting security and privacy. In: Auto-ID Labs Research Workshop (2004)
6. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic approach to “privacy-friendly” tags. In: Proc. of RFID Privacy Workshop (2003)
7. Molnar, D., Wagner, D.: Privacy and security in library RFID: Issues, practices, and architectures. In: Proc. of ACM CCS 2004, pp. 210–219 (2004)
8. Rhee, K., Kwak, J., Kim, S., Won, D.: Challenge-response based RFID authentication protocol for distributed database environment. In: Hutter, D., Ullmann, M. (eds.) SPC 2005. LNCS, vol. 3450, pp. 70–84. Springer, Heidelberg (2005)
9. Sarma, S., Weis, S., Engels, D.: RFID systems and security and privacy implications. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 454–470. Springer, Heidelberg (2003)
10. Cui, Y., Kobara, K., Matsuura, K., Imai, H.: Lightweight asymmetric privacy-preserving authentication protocols secure against active attack. In: Proc. of PerSec 2007 (2007)
11. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: Public key cryptography for RFID-tags. In: Proc. of PerSec 2007 (2007)
12. McLoone, M., Robshaw, M.: Public key cryptography and RFID tags. In: Abe, M. (ed.) CT-RSA 2007. LNCS, vol. 4377, Springer, Heidelberg (2006)
13. Shieh, W.G., Wang, J.M.: Efficient remote mutual authentication and key agreement. *Computers & Security* 25(1), 72–77 (2006)

14. EPCGlobal: EPC Generation-1 Tag Data Standards version 1.1, <http://www.epcglobalinc.org/standards/>
15. EPCGlobal: Class-1 Generation-2 UHF Air Interface Protocol Standard version 1.0.9: "Gen 2", <http://www.epcglobalinc.org/standards/>
16. Nguyen Duc, D., Park, J., Lee, H., Kwangjo, K.: Enhancing security of EPCglobal gen-2 RFID tag against traceability and cloning. In: Proc. of Symposium on Cryptography and Information Security, Hiroshima, Japan (2006)
17. Kim, K.H., Choi, E.Y., Lee, S.M., Lee, D.H.: Secure EPCglobal Class-1 Gen-2 RFID system against security and privacy problems. In: Meersman, R., Tari, Z., Herrero, P. (eds.) On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops. LNCS, vol. 4277, pp. 362–371. Springer, Heidelberg (2006)
18. Feldhofer, M., Rechberger, C.: A case against currently used hash functions in RFID protocols. In: Proc. of RFIDSec 2006 (2006)
19. Yksel, K., Kaps, J., Sunar, B.: Universal hash functions for emerging ultra-low-power networks. In: Proc. of CNDS 2004 (2004)
20. Wang, X., Feng, D., Lai, X., Yu, H.: Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. Cryptology ePrint Archive, Report 2004/199 (2004)
21. Wang, X., Lisa Yin, Y., Yu, H.: Finding collisions in the full SHA-1. In: Proc. of CRYPTO 2005, pp. 17–36 (2005)
22. Hernandez-Castro, J., Estevez-Tapiador, J., Ribagorda-Garnacho, A., Ramos-Alvarez, B.: Wheedham: An automatically designed block cipher by means of genetic programming. In: Proc. of CEC 2006, pp. 192–199 (2006)
23. Walker, J.: Randomness Battery (1998), <http://www.fourmilab.ch/random/>
24. Marsaglia, G., Tsang, W.: Some difficult-to-pass tests of randomness. Journal of Statistical Software 7(3), 37–51 (2002)
25. Suresh, C., Charanjit, J., Rao, J., Rohatgi, P.: A cautionary note regarding evaluation of AES candidates on smart-cards. In: Second Advanced Encryption Standard (AES) Candidate Conference (1999)
26. Lohmann, T., Schneider, M., Ruland, C.: Analysis of power constraints for cryptographic algorithms in mid-cost RFID tags. In: Domingo-Ferrer, J., Posegga, J., Schreckling, D. (eds.) CARDIS 2006. LNCS, vol. 3928, pp. 278–288. Springer, Heidelberg (2006)
27. Hell, M., Johansson, T., Meier, W.: Grain - a stream cipher for constrained environments. In: Proc. of RFIDSec 2005 (2005)
28. Roberts, C.: Radio frequency identification (RFID). Computers and Security 25(1), 18–26 (2006)

APPENDIX A

A Hash Tav-128 Ansi C and Statistical Tests

```

/*****/
Process the input a1 modifying the
accumulated hash a0 and the state
/*****/
void tav(unsigned long *state, unsigned long
*a0, unsigned long *a1)

{
unsigned long h0,h1;
int i,j,r1,r2,nstate;

/* Initialization */
r1=32; r2=8; nstate=4;
h0=*a0; h1=*a0;

/* A - Function */
for(i=0;i<r1;i++){h0=(h0<<1)+((h0+(*a1))>>1);}
/* B - Function */
for(i=0;i<r1;i++){h1=(h1>>1)+(h1<<1)+h1+(*a1);}

/* C and D - Function */
for(j=0;j<nstate;j++){
for(i=0;i<r2;i++)
{
/* C - Function */
h0^=(h1+h0)>>3;
h0=((((h0>>2)+h0)>>2)+(h0<<3)
+(h0<<1))^0x736B83DC;
/* D - Function */
h1^=(h1^h0)>>1;
h1=(h1>>4)+(h1>>3)+(h1<<3)+h1;
} // round-r2
state[j]=h0;
state[j]^=h1;
} // state

/* a0 updating */
*a0=h1+h0;
}

/*****/
Initialization of the state and a0 with
random values obtained from www.random.org
/*****/
void init_state(unsigned long *state, unsigned
long *a0)

{
state[0]=0xa92be51d;
state[1]=0xba9b1ef0;
state[2]=0xc234d75a;
state[3]=0x845c2e03;
a0[0]=0x768c7e74;
}

```

Table 1. Results obtained with ENT

| Test | Tav-128 |
|--------------------------------|--------------------|
| Entropy | 7.999999 bits/byte |
| Compression Rate | 0% |
| χ^2 Statistic | 269.73 (50%) |
| Arithmetic Mean | 127.4993 |
| Monte Carlo π estimation | 3.14178848 (0.01%) |
| Serial correlation coefficient | -0.000073 |

Table 2. Results obtained with the Diehard suite

| Test | Tav-128 p-value |
|------------------------------------|-----------------|
| Birthday Spacings | 0.725 |
| | 0.868 |
| GCD | 0.229 |
| | 0.138 |
| Gorilla | 0.779 |
| Overlapping Permutations | 0.823 |
| | 0.849 |
| | 0.349 |
| | 0.897 |
| Ranks of 31×31 and 32×32 Matrices | 0.556 |
| | 0.241 |
| Ranks of 6×8 Matrices | 0.315 |
| Monkey Tests on 20-bit Words | 0.312 |
| Monkey Test OPSO, OQSO, DNA | OK |
| Count the 1's in a Stream of Bytes | 0.473 |
| Count the 1's in Specific Bytes | OK |
| Parking Lot Test | 0.235 |
| Minimum Distance Test | 0.580 |
| Random Spheres Test | 0.912 |
| The Squeeze Test | 0.487 |
| Overlapping Sums Test | 0.106 |
| Runs Up and Down Test | 0.147 |
| The Craps Test | 0.3211 |
| | 0.067 |
| | 0.775 |
| | 0.261 |
| Overall KS p-value | 0.826 |

Low-Cost and Strong-Security RFID Authentication Protocol*

JeaCheol Ha¹, SangJae Moon², Juan Manuel Gonzalez Nieto³, and Colin Boyd³

¹ Dept. of Information Security, Hoseo Univ., 336-795, Korea
jcha@hoseo.edu

² School of Electrical Eng. and Computer Science, Kyungpook National Univ.,
702-701, Korea
sjmoon@ee.knu.ac.kr

³ Information Security Institute, Queensland Univ. of Technology, GPO Box 2434,
Brisbane, QLD, 4001, Australia
{juamma, boyd}@isrc.qut.edu.au

Abstract. This paper proposes a low-cost and strong-security RFID protocol to reduce the computational load on both the back-end database and the tags in an RFID system. When desynchronization occurs as a result of a communication failure or malicious attack, the proposed protocol can recover synchronization between the database and the tag in the following session. Furthermore, the proposed protocol also satisfies most security requirements, including the strong privacy property defined by Juels and Weis, plus robustness against replay and spoofing attacks and forward security.

Keywords: RFID system, authentication, indistinguishability, traceability, strong-privacy.

1 Introduction

Radio Frequency Identification (RFID) systems are expected to replace optical barcodes due to many important advantages, such as their low cost, small size, fast identification, and invisible implementation within objects. An RFID system consists of three parts: RFID tags, an RFID reader, and back-end database. Yet, since the RFID reader communicates with the tags using RF interfaces, this insecure channel leaves an RFID system vulnerable to various attacks, such as eavesdropping, spoofing, replay attacks, traceability, and message interrupt attacks. Although a lot of research has already focused on solving the security problems of RFID systems, some existing RFID protocols still suffer from various security weaknesses, including authentication, location privacy, and resynchronization between two entities.

One solution to protect tags from these threats is secure authentication between the tag and the reader. However, due to tag's computational power and

* This research was supported by the MIC of Korea, under the ITRC support program supervised by the IITA(IITA-2007-C1090-0701-0026).

storage space, a low-cost authentication protocol is needed that takes account of the back-end server's capacity and tag's implementation limitations.

Initial attempts to resolve the RFID authentication problem between the tag and the reader involved physical technologies and included the 'Kill command' [11], 'Active jamming' [5], and 'Blocker tag' [5] approaches. Thereafter, Weis *et al.* [9,10,11] proposed a hash-lock protocol and randomized hash-lock protocol as cryptographic solutions. However, in the randomized hash-lock protocol, the identity of a tag, ID_k , is transmitted from the reader to the tag through an insecure channel in the final step of authentication, making it vulnerable to a replay attack, spoofing attack, and location tracing. Meanwhile, Henrici and Müller [2] proposed an ID variation protocol based on a hash function, making it secure against a replay attack, as the identity of a tag is refreshed in each session, yet location tracing is still compromised, as the tag's response remains constant until the next authentication session when desynchronization occurs [8]. Dimitriou [1] also proposed a lightweight RFID authentication protocol that enforces user privacy and protects against cloning. However, there is no method for recovering synchronization when a state of desynchronization occurs. More recently, Juels and Weis [4] suggested improvements to their hash-lock protocol and presented a simple, formal definition of strong privacy. While their scheme is now robust against several attacks, the computational load on the back-end database is heavy when authenticating a tag. In 2006, Lee *et al.* [6] proposed an RFID mutual authentication scheme that introduced forward security(or forward traceability) to an RFID system, then proved that their scheme was perfectly indistinguishable and almost forward secure. However, the computational load on the back-end database is still heavy when finding a specific tag's ID . The Advanced Semi-Randomized Access Control(A-SRAC) proposed by Lee and Verbauwhede [7] resolves the location tracing problem, forward security, replay attacks, and so on. Yet, this protocol is vulnerable to location tracing due to the constant response of a tag in the case of successive desynchronization attacks.

Accordingly, this paper proposes a low-cost and strong-security mutual authentication protocol for an RFID system. In the case of desynchronization between the back-end database and a tag, the proposed protocol is able to recover the synchronization and maintain a robust security. As the correct ID can be found based on just comparing the transmitted hash message and the hashed values in the database, the computational load on the back-end system is efficient. The proposed protocol is also secure against spoofing attacks, replay attacks, and desynchronization attacks, while also satisfying the strong privacy property recently defined by Juels and Weis [4].

The remainder of this paper is structured as follows. Section 2 explains the security properties of an RFID system. Section 3 then analyzes several existing RFID systems as regards their security and implementation efficiency. The proposed low-cost and strong-security mutual authentication protocol for a secure RFID system is presented in section 4, and its security and efficiency examined in section 5. Some final conclusions are then given in section 6.

2 Security Properties of RFID System

An RFID system usually consists of three elements: RFID tags, the RFID reader, and back-end database. The RFID reader communicates with the tags using an RF signal, then sends the collected message to the back-end database. Unfortunately, the channel between the reader and a tag is insecure, as it is based on wireless communication while the channel between the reader and the database is considered as secure.

2.1 Security Problems

Since the communication between the reader and the tag is performed using a wireless RF interface, the communicated data can easily be tapped by an attacker. The various security threats that can occur with an insecure channel are as follows.

- **Information leakage:** A user may not want certain information known by attackers, such as ownership of expensive products, identification of personal medicine, and so on. Therefore, information leakage is a fundamental RFID privacy problem.
- **Spoofing and replay attack:** The attacker can impersonate a legal tag or reader using the messages collected from the tag or replaying certain useful messages.
- **Desynchronization attack:** An adversary can create a desynchronization state between the tag and the reader by blocking certain transmitted messages. This abnormal state can occur in an *ID*-renewable RFID system. If one of emitted values from the tag in desynchronization state is constant, the tag can be easily traced, thereby compromising the location privacy.
- **Location tracing attack:** The adversary can seek some useful information on a tag's location trace. This attack is essentially applied to a rigid RFID system in which certain communication messages emitted from a tag in the current session are identical to those used in the previous session.

2.2 Security Requirements

Various security requirements are needed for secure RFID authentication, as identified in previous literature [3,6,9]. The information leakage problem can be easily solved by using an anonymous ID for each product, then checking whether or not it is in the database. If a tag's *ID* is always fixed, then it is suitable for a ubiquitous environment, as many separate databases can be used. Conversely, if a tag's *ID* is renewed in each session, then it is suitable for a single database system due to the *ID* updating.

To prevent a spoofing attack or replay attack, the protocol should satisfy an authentication requirement. Plus, in the case an adversary has the ability to impersonate a tag or a reader, a mutual authentication protocol is needed. If a

tag's response does not depend on any reader input, as shown in [11], the tag's messages can be used in a replay attack.

One of the aims of a desynchronization attack is to spoil a tag by disturbing the ID search in the database. The other powerful threat is location tracing by successive desynchronization. If an adversary continuously blocks certain legal messages in a wireless channel, a historical trace can be identified. After blocking a message from a tag in a previous session, an adversary can trace a tag by comparing the messages in the current and previous sessions.

Even though an adversary does not know a tag's ID , a target tag can still be traced if some specific tag message patterns are found, *e.g.*, the transmitted data is increased by one in every session, as for a counter. For perfect location privacy, an RFID system should satisfy both *indistinguishability* and *forward security*, where the former means that the values emitted by one tag should not be distinguishable from the values emitted by other tags, while the latter means even if an attacker obtains the secret data stored in a tag, the location of the tag can not be traced back using previous known messages, *i.e.*, disclosed data, or communication information.

3 Analysis of Several RFID Authentication Schemes

This section analyzes the problems of existing RFID authentication protocols: (1) protocol developed by Juels and Weis [4], (2) protocol developed by Lee *et al.* based on synchronized secret information [6], (3) lightweight challenge-response RFID authentication protocol(LCRP) of Dimitriou [1], and (4) advanced semi-randomized access control(A-SRAC) scheme of Lee and Verbauwhede [7].

3.1 Randomized Hash-Locks

Juels and Weis [4] recently proposed a simple, formal definition of strong privacy and suggested improvements to their hash-lock protocol. In the improved randomized hash-lock scheme, a reader sends a random number r_R then a tag transmits the value $r_T || h(r_R || r_T || ID)$, where r_T is a random number generated by the tag. The authors insist that their protocol provides strong privacy and can protect against a replay attack. Rhee *et al.* [8] independently proposed a challenge-response authentication protocol based on a hash function that is almost the same as the improved randomized hash-locks scheme. Their scheme is also robust against a spoofing attack, replay attack, and location tracing attack. Nonetheless, the scheme is still vulnerable to forward security, as the ID does not change every session. Plus, their protocol is inefficient in terms of the computational load, as the back-end database is required to perform on average $m/2$ hash operations for an ID search, where m is the number of ID s.

3.2 Scheme Based on Synchronized Secret Information

Lee *et al.* [6] proposed an RFID mutual authentication scheme that utilizes a hash function and synchronized secret information. This scheme offers the most

enhanced security properties with respect to user privacy, including resistance against tag cloning, allowing an additional hash operation. In particular, they introduced forward security (or forward traceability) to an RFID system, then proved that their scheme is perfectly indistinguishable and almost forward secure. However, the back-end database is required to perform about m hash operations to find the specific ID related to a tag.

3.3 Lightweight Challenge-Response Protocol: LCRP

Dimitriou [1] proposed a lightweight challenge-response RFID authentication protocol (LCRP) that guarantees user privacy and protects against cloning. This protocol is based on the use of a secret shared between a tag and the back-end database that is renewed to avoid tag tracing. However, since an attacker can block the final message transmitted from the reader to the tag, it can result in a state of desynchronization. The tag and back-end database update using different keys, as the back-end database renews the secret key, while the tag keeps the old value, which allows an attacker to make the target tag useless. In addition, an attacker can trace a tag by successively sending a query from the reader in a desynchronized state. As the tag will respond with the same message $H(ID_i)$ in which ID_i is fixed in a desynchronized session, the tag cannot satisfy indistinguishability. Therefore, this protocol is vulnerable to a location tracing attack.

3.4 Advanced Semi-Randomized Access Control: A-SRAC

Lee and Verbauwhede [7] proposed advanced semi-randomized access control, called A-SRAC, where the tag sends $H(ID)$, r_T , and $H(ID||r_R)$ as a response to the reader. The authors insist that A-SRAC resolves most security properties, such as location tracing, forward security, and replay attacks based on the use of a random number generator in the tags. However, the scheme is still vulnerable to location tracing, as a tag will respond to the same $H(ID)$ in the case the last message from the reader is not received due to a message interrupt, where *key* in their original paper is the same notation as ID . Therefore, this protocol is vulnerable to location tracing due to the constant response of a tag in the case of successive desynchronization attacks in a second or third pass. Furthermore, if an attacker sends a constant r_R , then a tag will transmit a constant $H(ID||r_R)$, which is used to distinguish it from other tags and trace the tag's location.

3.5 Privacy Vulnerability in LCRP and A-SRAC

Juels and Weis recently proposed a simple, formal definition of strong privacy that is useful for a fundamental analysis of RFID systems [4]. As such, this section applies the definition to check the vulnerabilities of previous protocols. The goal of the adversary in their experiment was to distinguish between two different tags. In other words, if an RFID system does not satisfy strong privacy,

an adversary can distinguish two different tags. They parameterize the number of *READERINIT* messages sent by an attacker using r , the number of computational steps performed by s , and the number of *TAGINIT* messages sent by t . In addition, the parameter k is a security parameter, such as the length of ID or a random number. More details are given in [4].

As now explained, the LCRP [1] and A-SRAC [7] protocols are both unfortunately vulnerable to attack as regards strong privacy, as an adversary can send a *TAGINIT* message and block certain messages in the 2nd or 3rd pass between the tag and the reader. The aim of this blocking is to interrupt the ID updating of the tag. After certain messages are blocked, the target tag can not update its ID value, thus the tag's message, such as $H(ID)$, in next session will be the same as the one generated in the previous session. As a result, an adversary can distinguish the target tag by comparing the messages emitted in the previous and current sessions. The simple adversarial algorithm in Fig. 1 demonstrates that neither of the above two schemes can achieve (r, s, t) -privacy for $t \geq 2$, $s \geq 2$ and $r \geq 1$.

| LCRP/A-SRAC Adversarial Algorithm |
|--|
| 1. In Phase 1(Learning Phase), adversary selects a pair of distinct tags T_i and T_j uniformly at random. |
| 2. Adversary sends a query together random number to T_i (sends a <i>TAGINIT</i>). Adversary stores some messages and interrupts for ID updating in tag T_i . |
| 3. Adversary submits T_i and T_j as its challenge candidates. |
| 4. In Phase 2(Challenge Phase), adversary initializes a protocol between T_b^* and reader. |
| 5. If adversary can receive a same message with stored one from a tag, he guesses $b = 0$, i.e. $T^* = T_i$. Else he guesses $b = 1$, i.e. $T^* = T_j$. |

Fig. 1. Adversarial algorithm for LCRP and A-SRAC

4 Low-Cost and Strong-Security Mutual Authentication Protocol

This section describes the proposed low-cost and strong-security mutual authentication protocol for an RFID system. It is usually assumed that the communication channel between R and DB is secure, while the communication channel between R and T is insecure, as it is based on an air interface.

4.1 Notations

The notations used for the entities and computational operations to simplify the description are as follows.

| Notation | Meaning |
|-------------|---|
| T | RFID tag or transponder |
| R | RFID reader or transceiver |
| DB | back-end database or back-end server |
| ID | identity of tag, k bits |
| HID | hashed value of ID , k bits |
| PID | previous identity of tag used in previous session, k bits |
| r_R | random number generated by reader R |
| r_T | random number generated by tag T |
| $Query$ | request generated by R |
| $SYNC$ | parameter used to check whether both T and DB succeeded in updating ID simultaneously or not, 1 bit |
| $H()$ | one-way hash function, $H : \{0, 1\}^* \rightarrow \{0, 1\}^l$ |
| \parallel | concatenation of two inputs |
| $?$ | comparison of two inputs |

4.2 Protocol Description

The back-end database DB manages the ID , hashed values HID , and PID for each T in the database field. According to the state of the tag's previous session, the DB finds the ID for the current session or PID used for the previous session by comparing the received P with the HID and PID . After authenticating T , the DB updates the tag's ID and transmits a message of authentication.

An RFID tag T emits $P = H(ID)$ or $P = H(ID\parallel r_T\parallel r_R)$ according to the state of $SYNC$ in response to a query from the R . If the T does not receive the last message from the R due to a communication malfunction or the verification procedure fails, the $SYNC$ state is set as 1 and the T responds with $P = H(ID\parallel r_T\parallel r_R)$ to the R in the next session. In the case the protocol finishes normally, the $SYNC$ state becomes 0 and the T transmits $P = H(ID)$ in the next session.

The RFID reader R broadcasts a query to a T with a random number r_R and receives information related to authentication from the T , such as hashed values and a random number r_T . The message received from the T is then forwarded to the DB . After the DB authenticates the T , the R transmits the message received from the DB to the T . Fig. 2 shows the process of the proposed low-cost and strong-security protocol, and the following is a detailed description of each step:

1. The R generates a random number r_R and broadcasts it to a T using a $Query$.
2. The T chooses a random number r_T and computes P differently according to the state of $SYNC$. That is, if the $SYNC$ state is 0, then the T computes $P = H(ID)$, otherwise $P = H(ID\parallel r_T\parallel r_R)$ using r_T and r_R , and then sets the $SYNC$ state as 1. The T transmits P and r_T to the R , which then forwards the P and r_T messages to the DB together with r_R generated by itself in step 1.

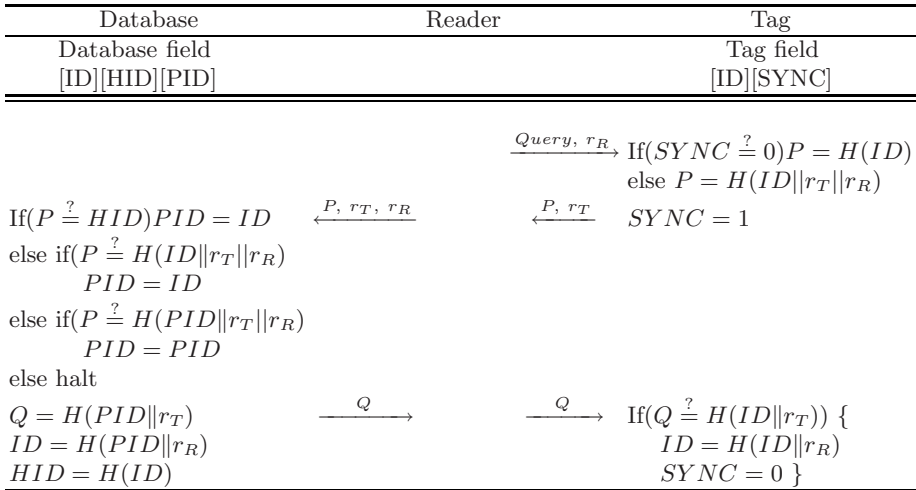


Fig. 2. The proposed low-cost and strong-security authentication protocol

3. The *DB* searches for the specific tag via the received *P*. First, the *DB* compares the received $P = H(ID)$ with the *HID* values saved in the database. If the values match, the *DB* regards the *ID* as the identity of the *T* requesting authentication. This is the general case when the previous session is closed normally. If the *DB* cannot find the *HID* in the first search, it computes a $H(ID||r_T||r_R)$ value for all the *ID* and compares it with the *P*. Thus, if the tag’s response messages were blocked in the previous session, that is, the *SYNC* state is 1 and the *ID*s in the *DB* and tag have not been updated, then the *DB* will find a match with the *ID* of the *T* in the second search. However, if the *DB* cannot find the *ID* of the tag in the above two cases, it computes a $H(PID||r_T||r_R)$ value for all the *PID* and compares it with the *P*. Thus, the *DB* will find a match with the *PID* of the *T* if the reader’s last messages were blocked in the previous session, that is, the *SYNC* state is 1 and the *DB* updated the *ID*, yet the tag’s *ID* was not updated. If the *DB* is still unable to find the tag’s *ID* using the above three cases, it halts the search for the *ID* and orders the *R* to query again. If the *DB* does find the *ID* or *PID* using one of the three search cases, it authenticates a tag by checking of the existence of an *ID*. The *DB* computes $Q = H(PID||r_T)$ and transmits it to the *R*, then computes $ID = H(PID||r_R)$ and updates $HID = H(ID)$ for the next session. The *R* then forwards the message *Q* to the *T*.
4. To verify the correctness of *Q* received from the *DB*, the *T* checks the following equation:

$$Q \stackrel{?}{=} H(ID||r_T). \tag{1}$$

¹ Since *ID* is updated into *PID* after finding the *ID* from *HID*, $Q = H(PID||r_T)$ is computed, regardless of the *PID* or *ID*.

If equation (1) is correct, the T updates its ID as $ID = H(ID||r_R)$, then sets the $SYNC$ state at 0.

5 Security and Efficiency

5.1 Basic Security Analysis

The basic security of the proposed protocol was analyzed against the attacks described in Section 2. To obtain secret information in a tag, an adversary must be able to compute the ID . However, any adversary cannot extract the ID value from $H(ID)$, $H(ID||r_T)$, or $H(ID||r_T||r_R)$ due to the one-way property of a hash function.

An adversary collects a tag's messages, then tries a spoofing attack based on impersonating a legitimate tag. However, an adversary cannot compute the transmitting message P without knowing the ID . On the other hand, to impersonate a reader, an adversary must send the correct Q to the tag. This is also impossible, because an adversary cannot compute it without knowing the ID value. A replay attack also cannot compromise the proposed protocol, as $H(ID)$ or $H(ID||r_T||r_R)$ is refreshed by updating the ID or including random numbers r_T and r_R in each session.

In the case of a desynchronization attack, where message loss occurs due to an adversary, the proposed protocol allows the tag and reader to recover synchronization. In the first case, if the adversary blocks the response messages transmitted from a tag, *i.e.*, step 2 in Fig. 2, plus, if the tag does not receive any correct response from the reader, the $SYNC$ state is set at 1, so the tag will transmit $H(ID||r_T||r_R)$ in the next session. Nonetheless, the two entities can recover their synchronization by searching the correct ID in the back-end database, as the DB stores the ID value. In the second case, if the adversary blocks the message Q which is transmitted from the reader, the DB has already updated the ID , yet the $SYNC$ state is set at 1. Therefore, when the tag transmits $H(ID||r_T||r_R)$ as the response in the next session, the T and DB can still recover synchronization based on finding the PID in the back-end database. Therefore, the proposed protocol can protect against a desynchronization attack.

For location tracing, the proposed protocol also guarantees location privacy based on renewing the ID for each session. After the authentication is completely closed in the previous session, the tag sends $H(ID)$ in response to a query in the current session. Thus, indistinguishability is satisfied as the ID in the previous session has been refreshed using a one-way hash function. In contrast, if the previous session is finished abnormally, the value P transmitted from the tag is $H(ID||r_T||r_R)$, thus the same response is not emitted by the tag in the subsequent session. Next subsection provides a formal proof of this indistinguishability, which is included in the strong-privacy definition presented by Juels and Weis [4].

In the case of forward security, it is assumed that an attacker obtains a tag's correct ID at some time. However, any previous ID cannot be extracted due

to the security property of the one-way hash function used to update the ID . Consequently, it is impossible for an attacker to trace the location of a tag backwards. However, it is harder to satisfy forward security during a state of successive desynchronization, during which an adversary collects all communication messages until obtaining the target secret ID . In this case, the adversary can trace the past history of the T , as the ID of the tag has not been changed. Nonetheless, the proposed protocol is able to guarantee forward security from the setup time to the latest point of successful ID updating.

5.2 Formal Proof of Strong Privacy(Indistinguishability)

The proposed protocol is able to guarantee strong privacy and is also resistant to other attacks. In particular, the proposed improvement of the LCRP and A-SRAC schemes is powerful for location tracing. Therefore, it is concluded that tags should not emit the same message as used in the previous session. Next, a formal proof is provided for the strong privacy [4] of the proposed protocol.

Theorem 1. ((r, s, t)-Private) *The proposed protocol is (r, s, t)-private in random oracle model, for any polynomially bounded adversary, i. e. any r, s, t polynomial in k .*

Proof: The simulator **Sim** is specified for T_b^* in the privacy experiment Exp^{priv} . Recall that the adversary chooses two challenge tags T_i and T_j . The adversary can collect the message list of P and r_T for a given random number r_R during the learning phase(Phase 1). Let L be the full list of pairs $\{(P, r_T)\}$ output by T_i and T_j . Let $O(\cdot)$ represent the random oracle for $H(\cdot)$ in this experiment.

During the challenge phase, **Sim** simulates the result of a TAGINIT call to T_b^* by generating a random number r_T of messages $\{(P, r_T)\}$ and appending then to a list L' . In order for the adversary to distinguish between the simulated challenge phase and a real challenge phase, the adversary should identify a pair $\{(P, r_T)\}$. It is assumed that the two tag ID s have fixed values, to allow them to be distinguished from each other. Consequently, one of the following three cases must occur at some time point during the experiment:

(1) To distinguish **Sim** from T_b^* in the message $P = H(ID)$, the adversary successfully submits to $O(\cdot)$ a query in the form of ID_i or ID_j , where $O(\cdot)$ is a random oracle. As the length of the ID s is k -bits, the corresponding space is 2^k . Yet, since the outputs do not reveal any information, the possibility that an adversary can successfully submit a query to $O(\cdot)$ is at most $2s/2^k$, where s is the number of computational steps for a random oracle.

(2) For a message $P = H(ID||r_T||r_R)$ that is transmitted in a state of desynchronization, the adversary has a success possibility of at most $(r + 2s + t^2)/2^k$ in which the space of P is also 2^k . It is why the random number r_R can be considered as fixed information in the experiment. In fact, the r_R can be intensively determined and transmitted to the tag by an adversary. The proof of possibility is given at [4] in the case of a randomized hash-lock protocol.

Thus, an adversary can distinguish **Sim** from T_b^* with a probability of at most $(r + 4s + t^2)/2^k$, which is negligible for a polynomially bounded adversary. Furthermore, for a successful replay attack, an adversary should guess the reader's random number r_R . Therefore, the success possibility is $1/2^k$, which is also negligible. \square

5.3 Comparison of Security

A security comparison with existing authentication protocols is described in Table 1. Most protocols are designed to protect against information leakage, spoofing attacks, and replay attacks. However, the LCRP [1] and A-SRAC schemes [7] do not satisfy the indistinguishability property in the case of a desynchronization attack that interrupts the updating of a tag's *ID*. This means that these schemes are unable to satisfy the strong privacy defined in [4], as shown in Fig. 1. Meanwhile, the Juels-Weis scheme *et al.* [4] and challenge-response-based protocol [8] do not satisfy forward security, as they use a fixed *ID*. In existing literature, this security weakness is present in most fixed *ID* RFID systems. Furthermore, Dimitrio's protocol [1] does not support resynchronization when a desynchronization attack occurs, which is a critical weakness in practical RFID systems. In a desynchronized state, a tag is useless and can not guarantee indistinguishability when a query by a malicious reader is repeatedly generated. In contrast, the proposed protocol is secure against most attacks presented up to now, including replay attacks, spoofing attacks, desynchronization attacks, and location tracing attacks. The proposed protocol also satisfies the strong privacy defined in [4].

Table 1. Comparison of security

| Protocol | LCRP [1] | Juels <i>et al.</i> [4] [8] | Lee <i>et al.</i> [6] | A-SRAC [7] | Proposed |
|------------------------|----------|-----------------------------|-----------------------|------------|----------|
| Information leakage | O | O | O | O | O |
| Spoofing attack | O | O | O | O | O |
| Replay attack | O | O | O | O | O |
| Indistinguishability * | × | O | O | × | O |
| Forward security | △ | × | △ | △ | △ |
| Resynchronization | × | O | O | O | O |

O : secure or support △ : partially secure × : insecure or not support.
 * : Strong privacy defined in [4].

5.4 Efficiency

When evaluating the computational cost for the two entities, the proposed protocol exhibited a remarkable enhancement for the *DB*, as shown in Table 2. Even though Lee *et al.* [6] and the challenge-response-based protocol [8] satisfy

most security items, except forward security, their critical disadvantage is that the *DB* is required to perform $m + 3$ or $m/2 + 2$ hash operations to authenticate a tag, where m is the number of *IDs*. In contrast, the proposed protocol only requires 3 hash operations by the *DB* and tag, respectively, and there is no relation with the length of m . In the case of just desynchronization, the correct *ID* or *PID* can be found based on an average of $m/2 + 3$ or $m + m/2 + 3$ hash operations. As such, the recovery time to a synchronized state is $m + 3$ operations on average. However, since desynchronization is a special and abnormal state, a usual synchronized state only requires 3 hash operations, which is a low computational cost compared to other existing protocols. Especially, the first response time of tag is just one hash operation, then the proposed protocol guarantees faster authentication in *DB* than LCAP or A-SRAC.

With the proposed protocol, since the *DB* only stores 3 *ID*-related values for each tag, the storage size of the *DB* is $3k \cdot m$, where k is the length of an *ID* or hashed value. Plus, a tag needs $(k + 1)$ -bits of memory to store its *ID* and 1-bit *SYNC* value. Plus, the total amount of messages transmitted from a tag to the reader is $2k$, and that from the reader to a tag is $2k$, except for a *Query*.

Table 2. Comparison of computational and communication efficiency

| Protocol | LCRP [1] | Juels <i>et al.</i> [4] [8] | Lee <i>et al.</i> [6] | A-SRAC [7] | Proposed |
|-----------------------------|--------------|-----------------------------|-----------------------|-------------|--------------|
| Comp.(hash # of <i>DB</i>) | 4 | $m/2 + 2$ | $m + 3$ | 4 | 3^* |
| Comp.(hash # of tag) | 4 | 2 | 3 | 4 | 3 |
| Storage of <i>DB</i> (bits) | $2k \cdot m$ | $k \cdot m$ | $3k \cdot m$ | $k \cdot m$ | $3k \cdot m$ |
| Storage of tag(bits) | k | k | k | k | $k + 1$ |
| Communication load | $5k$ | $4k^{**}$ | $4k$ | $6k$ | $4k$ |

m : the number of *IDs*.

* : $m + 3$ to recover the synchronization on average.

** : assuming that the 3-pass mutual authentication in [8] is adopted.

6 Conclusion

A low-cost and strong-security protocol was proposed to protect an RFID system from various existing attacks. The proposed protocol guarantees authentication, robustness against spoofing or replay attacks, and untraceability. Furthermore, even though the protocol can fall into a desynchronized state due to a malicious attacker, in which the database and a tag have different *IDs*, synchronization can be recovered in the next session. As regards its strong privacy property, a formal proof of the robustness of the proposed protocol is provided. In conclusion, the proposed protocol can be used in low-cost RFID systems that require a small computational load for both the back-end database and the tags.

References

1. Dimitriou, T.: A lightweight RFID protocol to protect against traceability and cloning attacks. In: SecureComm 2005. Security and Privacy for Emerging Areas in Communications Networks-2005, pp. 59–66 (September 2005)
2. Henrici, D., Müller, P.: Hash-based Enhancement of Location Privacy for Radio Frequency Identification Devices using Varying Identifiers. In: Proceeding of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp. 149–162. IEEE, Los Alamitos (2004)
3. Juels, A.: RFID: Security and Privacy: A Research Survey. RSA Laboratories (2005)
4. Juels, A., Weis, S.A.: Defining strong privacy for RFID, Cryptology ePrint Archive, Report 2006/137 Referenced (2006), at <http://eprint.iacr.org>
5. Juels, A., Rivest, R.L., Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for consumer Privacy. In: Proceeding of 10th ACM Conference on Computer and Communications Security 2003, pp. 103–111 (2003)
6. Lee, S., Asano, T., Kim, K.: RFID: Mutual Authentication Scheme based on Synchronized Secret Information. In: Proceedings of the SCIS 2006 (2006)
7. Lee, Y.K., Verbauwhede, I.: Secure and Low-cost RFID Authentication Protocols. In: AWiN. 2nd IEEE International Workshop on Adaptive Wireless Networks (November 2005)
8. Rhee, K., Kwak, J., Kim, S., Won, D.: Challenge-Response Based on RFID Authentication Protocol for Distributed Database Environment. In: Hutter, D., Ullmann, M. (eds.) SPC 2005. LNCS, vol. 3450, Springer, Heidelberg (2005)
9. Sarma, S.E., Weis, S.A., Engels, D.W.: Radio-Frequency Identification: Security Risks and Challenges. RSA Laboratories 6(1) (Spring 2003)
10. Weis, S.A.: Security and Privacy in Radio-Frequency Identification Devices. MS Thesis, MIT (2003)
11. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing. LNCS, vol. 2802, Springer, Heidelberg (2004)

A Ticket Based Binding Update Authentication Method for Trusted Nodes in Mobile IPv6 Domain

Ilsun You

School of Information Science, Korean Bible University,
205 Sanggye-7 Dong, Nowon-ku, Seoul, 139-791, South Korea
isyou@bible.ac.kr

Abstract. With the increasing usage of Mobile IPv6 in the mobile internet environment, the need of binding update authentication methods to protect malicious binding updates becomes more prevalent. The current authentication methods have tried to secure the binding update process between two previously unknown nodes on the assumption that no global security infrastructure available. However, the assumption is improper for a network domain where involved nodes can establish trust with each other. In this paper, for such a network domain, we propose a ticket based BU authentication method. Our proposed method achieves more efficient and secure binding update through tickets that are issued based on pre-established trust among the involved nodes.

1 Introduction

Mobile Internet Protocol version 6 (MIPv6), specified by IETF [1], is a protocol that enables nodes to stay reachable regardless of their movements and locations in the IPv6 Internet. In order to achieve mobility and reachability, this protocol let mobile nodes (MN) have two addresses: home address (HoA) and care-of address (CoA). Each MN belongs to a home network and is always identified by its HoA permanently allocated from its home network. While a MN visits a foreign network, it is associated with its CoA temporarily assigned by that network. The relation between the MN's HoA and CoA is called 'binding' for the MN. Whenever the MN changes its location, it must notify the home agent (HA), a router in the MN's home network, and the correspondent node (CN), the MN's peer node, of its new binding information. For this goal, the MN performs binding update (BU) processes with the CN as well as the HA. MIPv6 provides two possible modes for communications between the MN and the CN. The first mode, called bidirectional tunneling, deploys a HA as a trusted proxy for the MN in order that it may relay packets between the MN and the CN. However, such a triangle routing causes this mode to suffer from critical inefficiencies. For this mode, only the BU process between the MN and HA is needed. The second mode, called route optimization (RO), enables packets from the CN to be routed directly to the MN's CoA, thus eliminating the overhead resulted from tunneling via the HA. Before starting this mode, the MN should register its current binding

at both the HA and the CN by performing the BU processes. Since, unlike the MN-HA path protected by IPsec, the MN-CN path is insecure, without securing the BU process between the MN and the CN, this mode exposes the involved nodes to various security threats. In order to protect that BU process, the IETF provided the return-routability (RR) method [1], where the CN verifies the MN's HoA and CoA while sharing a secret with the MN. Despite its advantages, the method results in the performance and security problems [2-4]. In addition to the RR method, various approaches have been proposed based on the public key cryptography [2-13]. They use their own public key method to enable the MN and the CN to share a strong secret, the lifetime of which is sufficient long to minimize the amount of signaling messages and handover latency.

These current methods have tried to secure the BU process between two previously unknown nodes on the assumption that no global security infrastructure available. However, the assumption is improper for a network domain where involved nodes can establish trust with each other. Thus, more efficient method based on pre-established trust relationship is needed for such a network domain.

In this paper, we propose a ticket based BU authentication method, which enables the secure and efficient BU process for such a network domain. For this purpose, the proposed method uses a ticket that is issued based on pre-established trust among the involved nodes.

The rest of the paper is organized as follows. Section 2 reviews and analyzes the related works. In section 3, we propose a ticket based binding update authentication method. Section 4 analyzes the proposed method, which is then compared with other methods. Finally, section 5 draws some conclusions.

2 Related Works

Before starting the RO mode, a MN performs a BU process by sending a BU message to its CN, which then responds with a binding acknowledgement (BA) message. The fundamental requirement for securing the BU process is that the CN authenticates both the MN and its BU message. Unfortunately, it is so difficult to achieve strong authentication between two previously unknown nodes (MN and CN) where no global security infrastructure is available. Thus, the need has arisen for a security solution to enable sufficient authentication between the CN and the MN without traditional secret- or public key based authentication infrastructures.

Several researches have been conducted to address this security issue. The IETF has accepted the RR method as the standard for the secure BU process [1]. Besides the RR method, various approaches have been proposed based on the public key cryptography [2-13]. For exclusion of additional security infrastructure, they attempted to associate the MN's HoA with its public key through techniques such as Address Based Keys (ABKs) [14], Cryptographically Generated Address (CGA) [15] and Purpose-Built Keys (PBK) [16]. Recently, in order to improve security and inefficiency problems caused by the RR method, the Optimized Mobile IPv6 (OMIPv6) series have been researched and drafted into the network working group in IETF

[3-8]. Like other public key based approaches, the OMIPv6 series use their own public key techniques to construct a strong secret shared between the MN and the CN while optimizing the RR method.

These current methods have tried to accomplish the secure BU process between two previously unknown nodes on the assumption that no global security infrastructure available. Thus, they require no configuration and no trusted entities except for the MN's HA. However, the assumption is not suitable for a network domain where involved nodes can pre-establish trust relationship with each other. That is, more efficient method using pre-established trust can be applied for such a network domain. For such case, the IETF introduces the static shared key method, which requires the configuration of a shared secret between the MN and its CN [17].

In this section, we analyze the static shared key method after reviewing the RR method and the OMIPv6 series.

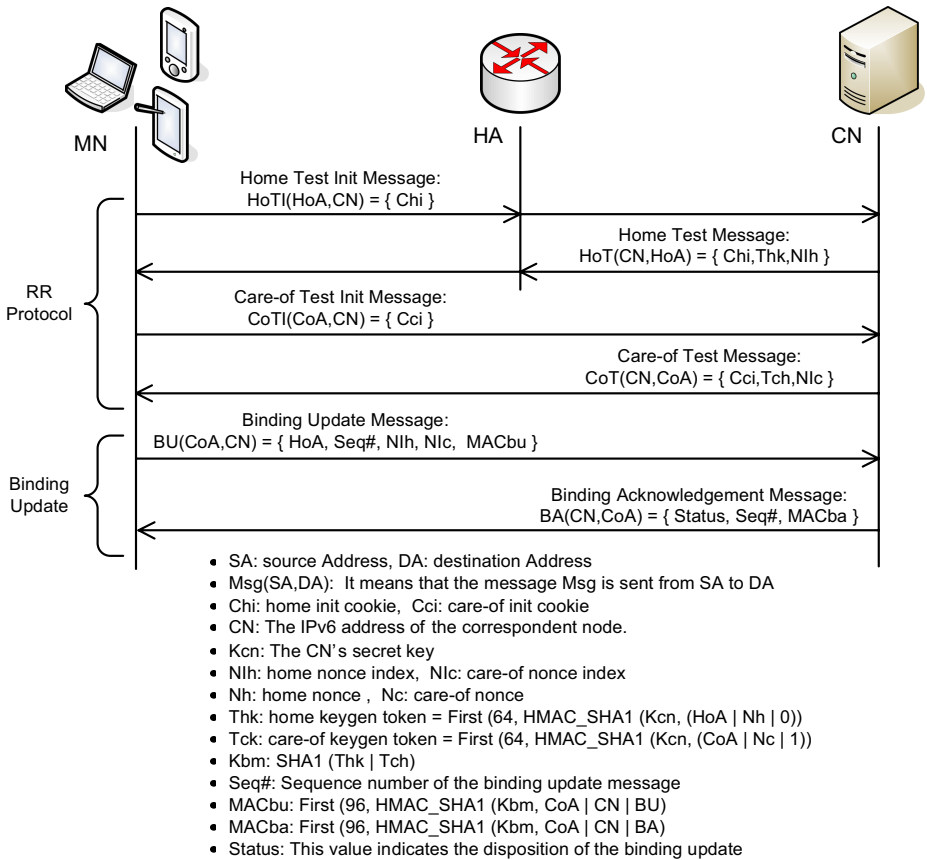


Fig. 1. The RR method

2.1 The Return Routability Method

The RR method enables the CN to verify if the MN is really reachable at its claimed CoA as well as at its HoA. Also, it allows the two nodes to establish a shared secret, which is then used to authenticate the BU and BA messages. Fig. 1 illustrates this method composed of the Home Test Init (HoTI), Care-of Test Init (CoTI), Home Test (HoT) and Care-of Test (CoT) messages. While the HoTI and HoT messages are relayed via the HA, the CoTI and CoT messages are directly exchanged between the MN and the CN. In order to start this method, the MN sends the HoTI and CoTI messages to its CN at the same time. In response to them, the CN transmits the MN the HoT and CoT messages, which include keygen tokens Thk and Tck. By hashing the tokens together, the MN builds a binding management key Kbm, and concludes the RR method. Derived from Thk and Tck, Kbm allows the CN to verify that the MN is addressable at its HoA and CoA. Thus, the key can be used to protect the subsequent BU process between the MN and the CN. After the RR method, the MN executes the binding process by exchanging the BU and BA messages with the CN.

Though this method satisfies the security requirements for the RO mode, it leads to the following problems [1-4]. First, because of security reasons, the Kbm's lifetime is limited to maximum 420 seconds. That makes Kbm updated at a high frequency, thus causing the number of mobility signaling messages and handover latency to be increased. Second, the method doesn't protect its messages on the MN-CN path as well as the HA-CN path. Such vulnerability exposes the RO mode to various security threats every few minutes during the ongoing session.

2.2 The OMIPv6 Series

The OMIPv6 series have been proposed to improve the security and inefficiency problems caused by the RR method. This series typically consist of the initial phase and the subsequent movement phase as shown in Fig. 2. The initial phase includes the RR test and BU steps. While the RR test step allows a MN to validate its own two addresses through the RR method, the BU step allows its CN to authenticate its public key, verify the BU message through the digital signature and establish the long-term key, Kbmperm. Since the CN has strong assurance about correctness of the MN's HoA during the phase, it can accept that the HoA test is eliminated from the successive binding processes. Thus, in the subsequent movement phase, the MN and its CN need to execute at most the CoA test before exchanging the BU and BA messages. In order to achieve the maximum efficiency, the first version of the OMIPv6 series [3] lets only the BU and BA messages communicated during the subsequent movement phase. But, that makes the first method vulnerable to redirection-based flooding attacks while not allowing the CN to verify the MN's CoA. To address this problem, the phase needs to include the CoA test, which results in a considerable effect on the amount of handover latency and signaling messages. Consequently, the OMIPv6 protocol series have tried to optimize the test as described in Table 1 [4, 7, 13].

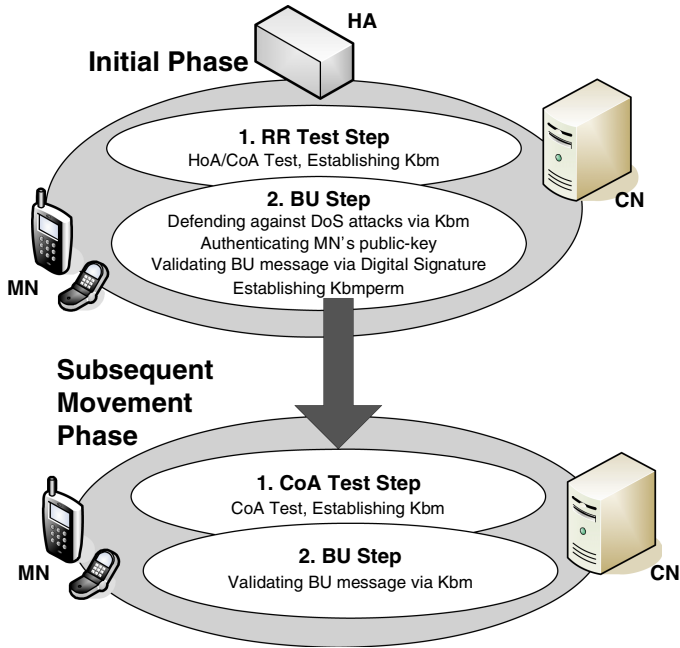


Fig. 2. The Route Optimization Mode of the OMIPv6 Series

Table 1. Comparison of subsequent movement phases of the OMIPv6 series

| Method | Technique for the CoA verification | Additional messages for the CoA verification | Latency until the MN starts to receive data packets |
|--------|--|---|---|
| (1) | CoA test | CoTI and CoT | 3 RTT |
| (2) | × | × | 1 RTT |
| (3) | CoA test | CoTI and CoT | 2 RTT |
| (4) | Early BU and CBA(credit-based authorization) | Early BU and BA messages including the CoA test option | 1 RTT (only if the complete BU process is successful) |
| (5) | CoA test delegation | - RtMoSol and RtMAck - Prefix Test Init (PreTI) and Prefix Test (PreT) | between 1 RTT and 2 RTT (except for the first BU process in the MN's access network infrastructure) |

* (1) The RR Protocol [1], (2) The OMIPv6 [5], (3) The OMIPv6-CGA Protocol [6], (4) The OMIPv6-CGA-CBA Protocol [8], (5) The CoA Test Delegation Protocol [13].

2.3 Static Shared Key Method

Recently, the IETF proposed the static shared key method for network environments where each MN can establish trust with its CNs [17]. In particular, this method is highly suitable for the case that MNs and CNs are administered within the same domain. As shown in Fig. 3, in this method, the MN and its CN pre-share key materials such as K_{cn} , nonces and nonce indexes, which are used for generating a Binding Management Key (K_{bm}). Through the preconfigured key materials, this protocol can omit signaling messages relating to the routability tests, thus minimizing the handover latency and the amount of signaling messages caused by the RR method.

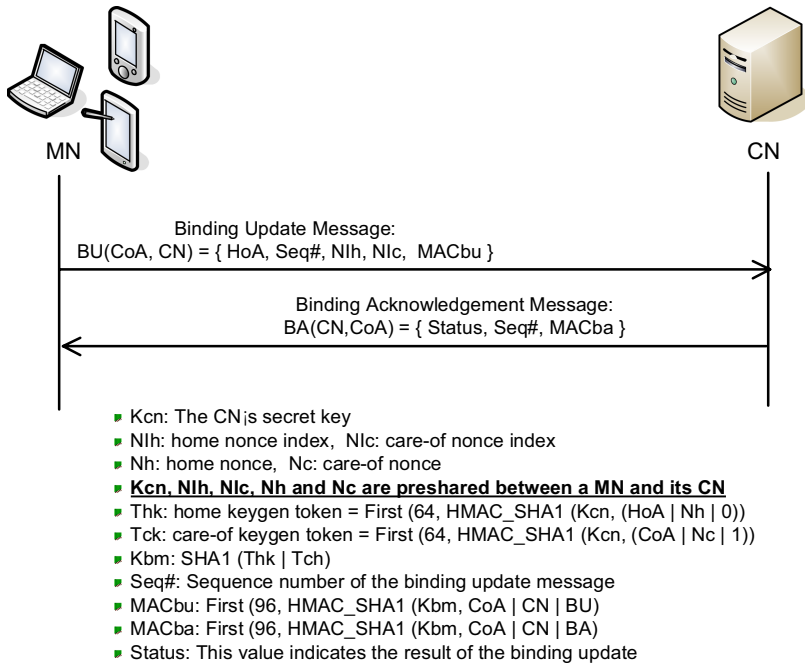


Fig. 3. Static Shared Key Method

Though this method achieves good efficiency, it has the following problems:

- Each CN needs the additional cost because it should preconfigure and maintain the key materials for its MNs. Such cost is more critical in an environment where every CN can be a MN.
- The elimination of the routability tests causes this method to be vulnerable to the redirection-based flooding attack, which the legitimate MN launches maliciously.
- This method depends on the sequence number $Seq\#$ to prevent the reply attack. When the sequence number rolls over, the involved nodes should configure new key materials.

3 Ticket Based Binding Update Authentication Method

In this section, we improve the static shared key method by employing a HA as a ticket issue server. For this goal, the proposed method requires the HA to pre-share a secret key with each CN. With such a pre-shared key, the HA securely distributes Kbmperm, a long-term key for binding management, between its MN and CN. That makes it possible for each MN to launch a binding update process with CNs, which establish trust relationship with its own HA. Thus, with the help of the HA playing a role of a ticket issue server, each CN can eliminate the cost for preconfiguring and maintaining the key materials for its MNs.

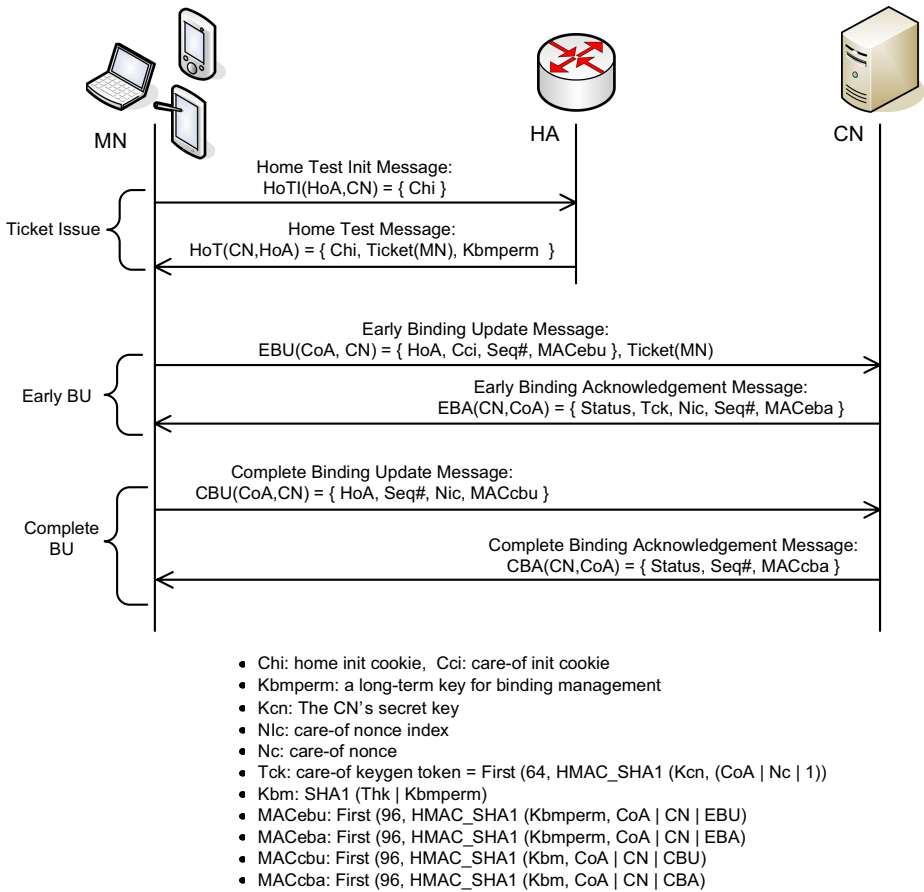


Fig. 4. Proposed Protocol

On the other hand, this method prevents the redirection-based flooding attacks by using the CoA test, which results in one additional round trip time (RTT) delay. Especially, in order to optimize the CoA test, it adopts the early binding update and credit-based authorization (CBA) techniques [7].

Fig. 4 shows the proposed method, which is divided into three phases as follows: ticket issue, early binding update and complete binding update phases.

Ticket Issue Phase: In this phase, when requested by the MN, the HA generates K_{bperm} , a long-term key for binding update, and issues a ticket including the generated key in encrypted form. The MN uses both the long-term key and the ticket to perform binding update with the CN. In order to initialize this method, the MN sends the CN a HoTI message, which is forwarded via the HA. When arriving at the MN's home-link, the message is intercepted by the HA, which then checks if there is a secret key pre-shared between itself and the CN. If such a key does not exist, the RR method is performed from this point. Otherwise, the HA generates K_{bperm} and issues a ticket for the MN. As depicted in Fig. 5, the ticket is composed of the MN's HoA, the HA's IPv6 address, the CN's IPv6 address, the life-time, EKey and MACticket. Especially, because EKey and MACticket are computed through K_{hc} , the CN having K_{hc} can verify the ticket and retrieve K_{bperm} from it. In stead of forwarding the HoTI message to the CN, the HA responds the MN with a HoT message including K_{bperm} and the ticket. Once the MN receives the ticket from the HA, the MN can omit this phase in each binding update process until its ticket is expired.

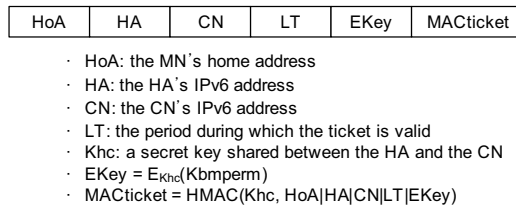


Fig. 5. Ticket Structure

Early Binding Update Phase: After the first phase, the MN and the CN execute the early binding update phase by exchanging the EBU and EBA messages. During the phase, the CoA test is applied to prevent the redirection-based flooding attacks. Especially, the CoA is performed in parallel with the data transmission from and to the MN's new CoA while minimizing the handover delay caused by itself. That is, the MN starts the data transmission immediately after sending the EBU message to the CN while the CN starts the data transmission immediately after sending the EBA message to the MN. In order to initiate the early binding update phase, the MN sends the CN the EBU message and its own ticket. When receiving them, the CN uses K_{hc} , a secret key pre-shared between itself and the HA, to verifies the ticket. If the verification is successful, the CN decrypts EKey with K_{hc} to retrieve K_{bperm} , which is then used to check if the EBU message is valid. In the case of the valid EBU message, the CN not only learns the MN's new CoA but also believes that the MN is the legitimate owner of the HoA. While starting using the new CoA from this time, the CN concludes this phase by sending the MN the EBA including Tck, a care-of keygen token.

Complete Binding Update Phase: After the second phase, in spite of knowing the MN's new CoA, the CN still cannot be sure that the MN is actually present at the new

address. Thus, the MN should prove that it is really reachable at its claimed CoA. For this goal, the MN performs the complete binding update phase. In order to start this phase, the MN sends the CN the CBU message, which can be authenticated through MAC_{cbu} computed with K_{bm} . Because K_{bm} is derived from T_{ck} in addition to K_{bperm} , the valid MAC_{cbu} lets the CN ensure that the MN receives the EBA message at its claimed CoA. Thus, if the CBU message is verified successfully, the CN believes the MN's presence at the new CoA. Finally, it concludes this phase by responding to the MN with the CBA message. As mentioned above, during the second phase, the data transmission is started though the MN's CoA is not verified. That causes the proposed method to be vulnerable to the misuse of unverified CoAs. To solve this security problem, the credit-based authorization (CBA) technique [7] is adopted. This technique limits the amount of the data transmission until the complete binding update phase finishes. In other words, if the amount of the data transmission is more than the specified value, the RO mode is postponed until the CBU message is verified successfully.

4 Analysis

This section analyzes the proposed method in terms of the management cost, the handover latency and the security. In particular, we focus on the management cost that each CN needs to preconfigure and maintain the key materials for its all MNs.

4.1 Management Cost

We use the following notations to derive the management cost of the proposed method.

- C_{MN} : the cost for the preconfiguration and maintenance of one node's key materials.
- C_{CN} : the management cost of all CNs
- C_{HA} : the management cost of the HA
- n : the number of MNs
- m : the number of CNs.
- o : the number of CNs that are a MN

The management cost of the static shared key method can be derived as follows:

$$C_{CN} = o(n-1)C_{MN} + (m-o)nC_{MN} = (on-o+mn-on) C_{MN} = (mn-o)C_{MN} \quad (1)$$

$$C_{HA} = nC_{MN} \quad (2)$$

$$C_{Total} = C_{CN} + C_{HA} = (mn+n-o)C_{MN} \quad (3)$$

The management cost of the proposed method can be derived as follows:

$$C_{CN} = mC_{MN} \quad (4)$$

$$C_{HA} = (n+m-o)C_{MN} \quad (5)$$

$$C_{Total} = C_{CN} + C_{HA} = (2m+n-o)C_{MN} \quad (6)$$

The difference between the proposed method and the static shared key method is as follows:

$$C_{Diff} = (mn+n-o)C_{MN} - (2m+n-o)C_{MN} = (n-2)mC_{MN} \tag{7}$$

According to the equation (7), we can know that if n is more than 2, the proposed method’s management cost is less than that of the static shared key method. Because in general the number of MNs is much more than 2, the proposed method is more efficient than the static shared key method in terms of the management cost.

4.2 Security

Redirection-Based Flooding Attack: During the early binding update phase, the proposed method executes the CoA test to defend against this attack. That is, through the care-of keygen token Tck included in the EBA message, the CN can check if the MN is actually present at its claimed CoA. Also, this method adopts the CBA technique to guard against the misuse of unverified CoAs. With this technique, the method controls the amount of data transmission from and to the unverified CoA during the period between the early binding update and complete binding update phases. Such a strategy optimizes the trade-off between security and efficiency.

Reply Attack: Because the HMAC values such as MACc_{bu}, MACc_{ba}, MACc_{bu} and MACc_{ba} are computed freshly through K_{bmperm} randomly generated by the HA as well as the sequence number Seq#, they enable this method to prevent the reply attack. Thus, though the sequence number rolls over, the involved nodes do not need to configure new key materials.

4.3 Handover Latency

In Table 2, we derive the handover latencies of the proposed method, the RR method and the static shared key methods. While the static shared key method, which runs the

Table 2. Handover latencies of the proposed method and others

| Method | | (1) | (2) | (3) | |
|------------------|-------------------------|---|--------------------------|---------------------------------|--------------------------|
| | | | | including the 1st phase | excluding the 1st phase |
| Handover Latency | L _{send} (RTT) | Max(RTT _{cot} , RTT _{hot}) = 2RTT | 0 RTT | 1RTT | 0 RTT |
| | L _{recv} (RTT) | Max(RTT _{cot} , RTT _{hot}) + 1RTT _{bu} = 3RTT | RTT _{bu} = 1RTT | 1RTT + RTT _{bu} = 2RTT | RTT _{bu} = 1RTT |

* (1) the RR method (2) the static shared key method (3) the proposed method

RTT_{cot}: the RTT for the CoA test (=1RTT),

RTT_{hot}: the RTT for the HoA test (=2RTT)

RTT_{bu}: the RTT for exchanging the BU and BA messages (=1RTT)

L_{send}: the latency until the MN starts to send data packets

L_{recv}: the latency until the MN starts to receive data packets.

binding update process without any address tests, has the optimized handover latency, the RR method including both the CoA and HoA tests has the worst handover latency. On the other hand, the proposed method can achieve the same handover latency as that of the static shared key method if the first phase is omitted. Because in most cases the proposed method runs without the first phase, it can provide the optimized performance.

5 Conclusions

In this paper, we propose a ticket based BU authentication method for a network domain where trust relationship can be established among involved nodes. Especially, we improve the static shared key method, which IETF introduces for such a network domain. For this goal, our proposed method employs a HA as a ticket issue server, which issues tickets based on pre-established trust. Such an employment requires the CN to make trust relationship with the HA instead of the MN, thus reducing the management cost of the CN. Also, our proposed method adopts the early binding update and CBA techniques in order to optimize the CoA test. Consequently, it is showed that our proposed method is efficient in terms of the management cost and security while achieving the almost same handover latency as that of the static shared key method.

References

1. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6, IETF RFC 3775 (June 2004)
2. Ren, K., Lou, W., Zeng, K., Bao, F., Zhou, J., Deng, R.H.: Routing optimization security in mobile IPv6. *Computer Networks* 50(13), 2401–2419 (2006)
3. You, I.: Improving the CGA-OMIPv6 Protocol for Low-Power Mobile Nodes. In: Gavrilova, M., Gervasi, O., Kumar, V., Tan, C.J.K., Taniar, D., Laganà, A., Mun, Y., Choo, H. (eds.) ICCSA 2006. LNCS, vol. 3983, pp. 336–343. Springer, Heidelberg (2006)
4. You, I., Lim, J.: Advanced Agent-Delegated Route Optimization Protocol for Efficient Multimedia Services at Low-Battery Devices. In: Cham, T.-J., Cai, J., Dorai, C., Rajan, D., Chua, T.-S., Chia, L.-T. (eds.) MMM 2007. LNCS, vol. 4352, pp. 479–486. Springer, Heidelberg (2006)
5. Haddad, W., Dupont, F., Madour, L., Krishnan, S., Park, S.: Optimizing Mobile IPv6 (OMIPv6), IETF Internet Draft, draft-haddad-mipv6-omipv6-01.txt (February 2004) (work in progress)
6. Haddad, W., Madour, L., Arkko, J., Dupont, F.: Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6), IETF Internet Draft, draft-haddad-mip6-cga-omipv6-04 (November 2005) (work in progress)
7. Arkko, J., Vogt, C., Haddad, W.: Enhanced Route Optimization for Mobile IPv6, IETF RFC 4866 (May 2007)
8. Dupont, F., Haddad, W.: Optimizing Mobile IPv6 (OMIPv6), IETF Internet Draft, draft-dupont-mipshop-omipv6-00.txt (February 2006) (work in progress)
9. O’Shea, G., Roe, M.: Child-proof authentication for MIPv6 (CAM). *ACM Computer Communications Review* 31(2) (April 2001)

10. Roe, M., Aura, T., O'Shea, G., Arkko, J.: Authentication of Mobile IPv6 Binding Updates and Acknowledgments, Internet Draft, draft-roe-mobileip-updateauth-02.txt, February 2002 (work in progress)
11. Montenegro, G., Castelluccia, C.: Crypto- Based Identifiers(CBIDs): Concepts and Applications. *ACM Transactions on Information and System Security* 7(1), 97–127 (2004)
12. You, I., Cho, K.: A Security Proxy Based Protocol for Authenticating the Mobile IPv6 Binding Updates. In: Laganà, A., Gavrilova, M., Kumar, V., Mun, Y., Tan, C.J.K., Ger-vasi, O. (eds.) *ICCSA 2004. LNCS*, vol. 3043, Springer, Heidelberg (2004)
13. Haddad, W., Krishnan, S., Dupont, F.: Mobility Signaling Delegation in OptiSEND, IETF Internet Draft, draft-haddad-mipshop-mobisig-del-02.txt (October 2006) (work in progress)
14. Okazaki, S., Desai, A., Gentry, C., et al.: Securing MIPv6 Binding Updates Using Address Based Keys (ABKs), IETF, draft-okazaki-mobileip-abk-01.txt (October 2002) (work in progress)
15. Aura, T.: Cryptographically Generated Addresses (CGA), IETF RFC 3972 (March 2005)
16. Bradner, S., Mankin, A., Schiller, J.: A Framework for Purpose-Built Keys (PBK), IETF Internet Draft, draft-bradner-pbk-frame-06.txt (October 2003) (Work in progress)
17. Perkins, C.: Securing Mobile IPv6 Route Optimization Using a Static Shared Key, IETF RFC 4449 (June 2006)

Author Index

- An, Sunshin 494
Anderson, Anne 69
Anderson, Jonathan S. 660
Atajanov, Merdan 309

Bae, Seokhoon 93
Boyd, Colin 557, 795
Busse, Marcel 579

Chadwick, David 69
Chang, Hangbae 22
Chang, Hsu-Sheng 205
Chang, Ing-Chau 365, 401
Chang, Yaotsu 617
Chao, Hsi-Lu 226
Chen, Chao-Lieh 321
Chen, Huiyan 704
Chen, Jeng-Yueng 297
Chen, Jian-Hong 617
Chen, Jian-Jia 604
Chen, Kefei 716
Chen, Kuan-yin 193
Chen, Ming-Hung 413
Chen, Qi 333
Chen, Shi-Feng 365
Chen, Shing-Kuang 215
Chen, Yi-Tsung 321
Chen, Zih-Heng 617
Cheng, Chun-Hua 638
Cheng, Shih-Yao 215
Cheng, Ya-Lien 285
Cheng, Zixue 377
Chi, Wei-Chieh 413
Cho, SeongJe 82
Cho, Yong-Man 455, 467
Choi, Jihoon 538
Choi, WoongChul 82
Chou, Chen-Fu 401
Chou, Cheng-Fu 413
Chou, Li-Der 215
Chun, Seung-Yong 515
Cooper, G.S. 69
Curley, Edward 660

Dohi, Tadashi 31
Dong, Mianxiong 377

Effelsberg, Wolfgang 579
Erdogan, Senol Zafer 389
Estevez-Tapiador, Juan M. 781

Feng, Dan 341
Fuchs, Markus 579

Green, Dale 474
Gritzalis, Stefanos 12
Grumer, Matthias 627
Guo, Minyi 377

Ha, JeaCheol 557, 795
Haenselmann, Thomas 579
Han, Byungwan 22
Han, Jong Wook 124
He, Fei 341
Hernandez-Castro, Julio Cesar 781
Ho, Chang-Yang 226
Hong, Jinkeun 146
Hou, Ting-Wei 435
Hsu, Chih-Cheng 413
Hsu, Kai-Cheng 249
Hu, Junn-Yen 401
Huang, ChingYao 193
Huang, Hui-Feng 550
Huang, Shih-Hsu 638
Huang, Sze-Wei 237
Huang, Yu-Kai 237
Huang, Zheng-Yi 136
Hung, Kun-Chien 181
Hung, Yi-Hsuan 435
Hussain, Sajid 1, 389, 745
Hwang, Yuan-Chu 57

Jensen, E. Douglas 660
Jing, Ming-Haw 617
Juang, Wen-Shenq 728

Kang, Bo Gyeong 686
Kang, Sukhoon 93
Kang, SukJoong 82
Karyda, Maria 12
Kausar, Firdous 1, 745
Kebemou, Augustin 674
Ker, Jar-Shone 321

- Kim, Changhwa 455, 467, 523
 Kim, Chungsan 445
 Kim, Daeyoung 568
 Kim, Eunchan 445
 Kim, Geon Woo 124
 Kim, HwanKoo 557
 Kim, Hyoungshick 425
 Kim, Ki-Man 515
 Kim, Kihong 146
 Kim, Kiseon 445
 Kim, Moonoh 22
 Kim, Sangkyung 455, 467, 523
 Kim, Sang Wook 124
 Kim, Se-Young 515
 Kim, Taehong 568
 Kim, Tai-hoon 1
 Kim, Youngsoo 568
 Kimura, Masahiro 355
 King, Thomas 579
 Kinoshima, Takashi 355
 Kobayashi, Kazutaka 355
 Kuo, Tei-Wei 604
 Kuo, Yau-Hwang 321
 Kwon, Hyuk-jun 22
- Lai, Chung-Yi 401, 413
 Lee, Deok Gyu 124
 Lee, Eunseok 158
 Lee, Jeng-Wei 321
 Lee, Seung-Jae 455, 467
 Lee, Seungjae 523
 Lee, Wonjun 538
 Lee, YongSuk 82
 Lee, Youn-Tai 181
 Lee, Yung-Hen 604
 Lei, Chin-Laung 728
 Lei, SuTe 592
 Li, Chien-Yi 215
 Li, Jianhua 716
 Li, Ping 770
 Li, Xiangxue 716
 Lin, Cheng-Zh 321
 Lin, David W. 181
 Lin, Pochun 261
 Lin, Yaping 770
 Lo, N.W. 43
 Lu, Yongqian 115
- Masood, Ashraf 1, 745
 Matsumoto, Noriko 355
- Mbanaso, U.M. 69
 Men, Chaoguang 115
 Mohan, Anand 169
 Moon, SangJae 557, 795
 Mühlberger, Andreas 627
- Nam, Heungwoo 494
 Neffe, Ulrich 627
 Ng, Joseph K. 273
 Nguyen, Hung Trong 482
 Nieto, Juan Manuel Gonzalez 557, 795
- Oh, S. Jae 425
 Ota, Kaoru 377
- Pang, Ai-Chun 237
 Park, JeaHoon 557
 Park, Je Hong 686
 Park, Jeongmin 158
 Park, Jong Hyuk 12, 389, 745
 Park, Soo-Hyun 482, 505, 531
 Peris-Lopez, Pedro 781
 Piao, Shunshan 158
- Ravindran, Binoy 660
 Ribagorda, Arturo 781
- Schieferdecker, Ina 674
 Sha, Edwin 592
 Sha, Min-Shi 401
 Shao, Zili 103
 Sheu, Shiann-Tsong 205
 Shih, Yung-Chien 249
 Shimokawa, Toshihiko 309
 Shin, Soo-Young 482, 505, 531
 Song, Yu 333
 Steger, Stefan Lickl Christian 627
 Stojcevski, Alex 169
 Su, JinShu 103
 Sung, Jongwoo 568
- Tan, Zhipeng 341
 Tsao, Shiao-Li 261, 285
 Tseng, Chien-Chao 249
 Tseng, Li-chuan 193
- Uemura, Toshikazu 31
- Wang, Dongsheng 115
 Wang, Hai-wei 181
 Wang, Kuochen 261

- Wang, Pang-Chieh 435
Wang, Ren-Chiun 728
Wang, Sheng-De 136
Wang, Zhu 704
Weiss, Reinhold 627
Wendt, Manuel 627
Woo, Seok 445
Wu, Jiaying 770
- Yan, Xia 103
Yang, Chih-Chen 205
Yang, Chun-Chuan 297
Yao, Kai-chao 648
Yeh, Kuo-Hui 43
Yen, Wei-Ting 638
Yeung, Wilson M. 273
Yoo, Kee-Young 758
Yoo, Seongeun 568
Yoon, Eun-Jun 758
- Yoshida, Norihiko 309, 355
You, Ilsun 808
Yu, Li-Sheng 297
Yuan, Soe-Tsyr 57
Yun, Phil-Jung 455
- Zakaria, Nurul Azma 355
Zayegh, Aladin 169
Zeng, YingZhi 103
Zhang, Fangguo 692
Zhang, Futai 692
Zhang, Kang 592
Zhang, Lei 692
Zhao, BaoKang 103
Zheng, Dong 716
Zheng, Sixian 261
Zhou, JunYang 273
Zhou, Ke 341