Periklis Chatzimisios
Christos Verikoukis
Ignacio Santamaría
Massimiliano Laddomada
Oliver Hoffmann (Eds.)

LNICST

45

Mobile Lightweight Wireless Systems

Second International ICST Conference, MOBILIGHT 2010
Barcelona, Spain, May 2010
Revised Selected Papers

ICST

Springer

Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering 45

Editorial Board

Ozgur Akan
Middle East Technical University, Ankara, Turkey
Paolo Bellavista
University of Bologna, Italy
Jiannong Cao
Hong Kong Polytechnic University, Hong Kong
Falko Dressler
University of Erlangen, Germany
Domenico Ferrari
Università Cattolica Piacenza, Italy
Mario Gerla
UCLA, USA
Hisashi Kobayashi
Princeton University, USA
Sergio Palazzo
University of Catania, Italy
Sartaj Sahni
University of Florida, USA
Xuemin (Sherman) Shen
University of Waterloo, Canada
Mircea Stan
University of Virginia, USA
Jia Xiaohua
City University of Hong Kong, Hong Kong
Albert Zomaya
University of Sydney, Australia
Geoffrey Coulson
Lancaster University, UK

Periklis Chatzimisios Christos Verikoukis
Ignacio Santamaría Massimiliano Laddomada
Oliver Hoffmann (Eds.)

Mobile Lightweight Wireless Systems

Second International ICST Conference
MOBILIGHT 2010
Barcelona, Spain, May 10-12, 2010
Revised Selected Papers

Springer

Volume Editors

Periklis Chatzimisios
Technological Educational Institution of Thessaloniki, Department of Informatics
57400 Sindos, Thessaloniki, Greece
E-mail: pchatzimisios@ieee.org

Christos Verikoukis
Centre Tecnològic de Telecomunicacions de Catalunya
Parc Mediterrani de la Tecnologia, 08860 Castellfels, Barcelona, Spain
E-mail: cveri@cttc.es

Ignacio Santamaría
Universidad de Cantabria, Dpto. Ingeniería de Comunicaciones
39005 Santander, Spain
E-mail: nacho@gtas.dicom.unican.es

Massimiliano Laddomada
Texas A&M University, Texarkana, TX 75505-5518, USA
E-mail: mladdomada@tamut.edu

Oliver Hoffmann
TU Dortmund, Lehrstuhl für Kommunikationstechnik
Otto-Hahn-Str. , 44221 Dortmund, Germany
E-mail: oliver.hoffmann@tu-dortmund.de

Library of Congress Control Number: 2010937768

CR Subject Classification (1998): C.2, D.2, C.4, K.6.5, C.2.4, D.4.4

ISSN 1867-8211
ISBN-10 3-642-16643-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-16643-3 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.com

© ICST Institute for Computer Science, Social Informatics and Telecommunications Engineering 2010
Printed in Germany

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

Foreword

Following the success of the First MOBILIGHT 2009 in Athens, Greece, the Second International Conference on Mobile Lightweight Systems (MOBILIGHT) was held in Barcelona, Spain on May 10-12, 2010.

It was not an easy decision to carry on organizing a scientific event on wireless communications, where competition is really enormous. This decision was motivated by discussion with many colleagues about the current unprecedented demand for lightweight, wireless communication devices with high usability and performance able to support added-value services in a highly mobile environment. Such devices follow the users everywhere they go (at work, at home, while travelling, in a classroom, etc.) and result in exciting research, development and business opportunities. Such scenarios clearly demand significant upgrades to the existing communication paradigm in terms of infrastructure, devices and services to support the “anytime, anywhere, any device” philosophy, providing novel and fast-evolving requirements and expectations on research and development in the field of information and communication technologies. The core issue is to support wireless users' desire for 24/7 network availability and transparent access to "their own" services.

In this context, we continue to envision an international forum where practitioners and researchers coming from the many areas involved in lightweight wireless systems’ design and deployment would be able to interact and exchange experiences. For this reason, MOBILIGHT was again targeted toward information exchange and cross-fertilization among the different worlds of academia, research centers and industry through the organization of specific and interacting tracks related to: (1) technology, including wireless (WPAN, WLAN, WMAN/cellular) as well as architectures and design methodologies to support seamless access to the communication facility; (2) services, in the vision of “always on” requirement; (3) business models, opportunities and solutions.

The Technical Program Committee of MOBILIGHT 2010 gathered more than 60 leading scientists and was assisted by at least 30 additional external reviewers, originating from more than 20 countries worldwide. More than 100 registered participants attended MOBILIGHT 2010. The conference attracted more than 90 submissions, and the final technical program encompassed 65 high-quality research papers organized in three workshops and ten special sessions, most of them including up-to-date results from research projects funded by the European Commission (NEWCOM++, REWIND, MIMAX, OMEGA, SELF-NET, ICARUS, MOBILIA, INSPIRE). All submitted papers were peer-reviewed by at least three independent reviewers (including two TPC members) to ensure high quality and standards.

The technical program of MOBILIGHT 2010 also included four plenary talks by internationally recognized industrial and academic leaders, covering up-to-date research and development topics, as well as funding opportunities within the international and European research communities. Moreover, the technical program included two tutorials focused on a machine-to-machine communication paradigm in addition to basics and future developments of radio communications. Finally, two panels took place in order to provide discussion between the audience and top-level experts from research and industry. Selected topics for this year were "Wireless Communications for Improving Security in High-Speed Railway Transportation Systems" and "Future and Applications of Wireless Mesh Networks."

We would like to express our gratitude to all the people of the organizing committee for their hard teamwork and true dedication. In particular, our gratitude goes to the Technical Co-chairs, Ignacio, Massimiliano and Oliver, for their constant support and fruitful suggestions, to ICST and CREATE-NET for providing technical and financial sponsorship of the event and, last but not least, to Prof. Imrich Chlamtac for his precious suggestions and his vision. But most of all, we would like to thank the authors and contributors for trusting the organizing committee and giving us the chance to set up a high-level technical program. Lastly, we are very grateful for all the hard work done and the support offered by all the reviewers for the thorough review reports and constructive remarks aimed ensuring at high technical quality.

The conference proceedings are published by Springer and will be available in Springer's *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (LNICST). Selected high-quality papers will be invited to special issues in prestigious international journals. Detailed information and photos are available at the conference website, http://www.mobilight.org .

We are looking forward to meeting you at the next MOBILIGHT 2011 that will be held in Bilbao (Basque Country), Spain, in May 2011.

Periklis Chatzimisios
Christos Verikoukis

Organization

Steering Committee

Imrich Chlamtac	CREATENET, Italy
Fabrizio Granelli	University of Trento, Italy
Charalabos Skianis	University of Aegean, Greece

Conference General Chairs

Periklis Chatzimisios	Alexander TEI of Thessaloniki, Greece
Christos Verikoukis	CTTC, Spain

Technical Program Chairs

Ignacio Santamaría	University of Cantabria, Spain
Massimiliano Laddomada	Texas A&M University-Texarkana, USA
Oliver Hoffmann	Dortmund University of Technology, Germany

Tutorial Chair

Ana García Armada	Universidad Carlos III de Madrid, Spain

Special Sessions / Workshop Chairs

Ioannis Chochliouros	OTE, Greece
Javier Del Ser	ROBOTIKER-Tecnalia, Spain

Publications Chair

Jesús Alonso	Zárate CTTC, Spain

Publicity Co-chairs

Marco Di Renzo	CNRS, France
Nizar Zorba	University of Jordan, Jordan
Thomas Lagkas	University of Western Macedonia, Greece

Panel Chair

Luis Alonso	Universitat Politècnica de Catalunya, Spain

Local Arrangements Chairs

Elli Kartsakli	Universitat Politècnica de Catalunya, Spain
Ferran Adelantado	Universitat Oberta de Catalunya, Spain
David Sanchez	Universitat Pompeu Fabra, Spain

Conference Coordinator

Gergely Nagy	ICST

Web Chair

Eirini Karapistoli	Aristotle University of Thessaloniki, Greece

Technical Program Committee

Chadi Assi	Concordia University, Canada
Albert Banchs	Universidad Carlos III de Madrid, Spain
Paolo Bellavista	University of Bologna, Italy
Daniele Borio	University of Calgary, Canada
Christos Bouras	University of Patras, Greece
Luis Castedo	University of A Coruña, Spain
Andrea F. Cattoni	DIBE - University of Genoa, Italy
Hsiao-Hwa Chen	National Cheng Kung University, Taiwan
Chang-Soon Choi	IHP, Germany
Pedro Crespo	CEIT, Spain
Tasos Dagiuklas	TEI of Messologgi, Greece
Fred Daneshgaran	California State University, Los Angeles, USA
Dimitris Dernikas	AIRCOM International, UK
Ralf Eickhoff	Dresden University of Technology, Germany
Chuan Heng Foh	Nanyang Tech. University, Singapore
Michael Georgiades	Infostrada Communications, Cyprus
Victor Govindaswamy	Texas A&M University-Texarkana, USA
Fabrizio Granelli	DISI - University of Trento, Italy
Jussi Haapola	CWC, Finland
Athanasios Kanatas	University of Piraeus, Greece
Helen Karatza	Aristotle University of Thessaloniki, Greece
Tom Karygiannis	National Institute of Standards & Tech, USA
Dzmitry Kliazovich	DISI - University of Trento, Italy
George Kormentzas	University of Aegean, Greece
Yevgeni Koucheryavy	Tampere University of Technology, Finland
Fotis Lazarakis	NCSR Demokritos, Greece

Michael D. Logothetis	DECE - University of Patras, Greece
Pascal Lorenz	University of Haute Alsace, France
Stefan Mangold	Swisscom, Switzerland
Sebastian Max	RWTH Aachen University, Germany
Marina Mondin	Politecnico di Torino, Italy
Ioannis Moscholios	University of Peloponnese, Greece
Qiang Ni	Brunel University, UK
Stefan Nowak	Dortmund University of Technology, Germany
Kostas Pentikousis	VTT, Finland
Christos Politis	Kingston University, UK
Simone Redana	Nokia Siemens Networks, Germany
Holger Rosier	RWTH Aachen University, Germany
Isabelle Siaud	France Telecom, France
Harry Skianis	University of Aegean, Greece
John Soldatos	Athens Information Technology, Greece
Ilenia Tinnirello	University of Palermo, Italy
Andrea Tonello	University of Udine, Italy
Jose Miguel Torres Avanzit	Spain
Dimitrios D. Vergados	University of Piraeus, Greece
Javier Via	University of Cantabria, Spain
Vasileios Vitsas	TEI of Thessaloniki, Greece
Luca Vollero	Universita Bio-Medico di Roma, Italy
Yang Xiao	University of Alabama, USA
Nizar Zorba	University of Jordan, Jordan
Gil Zussman	Columbia University, USA
Lambros Sarakis	NCSR Demokritos, Greece
Nikos Dimitriou	University of Athens, Greece
Costantinos	Voudouris TEI Athens, Greece
Panagiotis Tsiakas	TEI Athens, Greece
Fernando López	Telefónica I+D, Spain
Sergio Gil-López	ROBOTIKER, Spain
Iraide Unanue	ROBOTIKER, Spain
Andrea Blanco	ROBOTIKER, Spain
Jose Mari Cabero	ROBOTIKER, Spain
Enrique Areizaga	ROBOTIKER, Spain
Askoxilakis Ioannis	FORTH, Greece
Paulo Marques	ICTI, Portugal
Simona Halunga	University "Politehnica" of Bucharest, Romania
Kandeepan Sithamparanathan	CREATNET, Italy
Maciej J. Nawrocki	Wroclaw Research Center EIT, Poland
Jorge Garcia	UPC, Spain
Sherali Zeadally	University of the District of Columbia, USA

EUMOBILE 2010 – Organizers

Tasos Dagiuklas	TEI of Mesolonghi, Greece
Christos Politis	Kingston University, UK

PHYLOM 2010 – Organizers

Sergio Gil-Lopez	Tecnalia-Telecom, Spain
Sancho Salcedo-Sanz	University of Alcala Escuela Politécnica Superior, Spain

UAS 2010 – Organizers

Ondrej Krejcar	Technical University of Ostrava Centre for Applied Cybernetics, Czech Republic
Jiri Horak	Technical University of Ostrava Institute of Geoinformatics, Czech Republic
Marek Penhaker	Technical University of Ostrava Centre for Applied Cybernetics, Czech Republic

Table of Contents

MobiLight 2010 – Special Session on "Mobility Concepts and IMT-Advanced (MOBILIA)"

Performance of MC-DS-CDMA System in Rayleigh Fading Channel with Non-coherent Combining Schemes and MAI Interference 1
Ismahene Ikhlef, Abdellatif Said, Faouzi Soltani, and Faouzi Bader

Spectral Efficiency Using Combinations of Transmit Antenna Selection with Linear Dispersion Code Selection 11
I. Gutierrez and F. Bader

A Reconfigurable Power Amplifier for Mobile WIMAX Applications 22
Yolanda Fernández, Miguel Ángel Peña, and Francisco Díaz

An Access Selection Prototype Based on IEEE 802.21 31
Bruno Cendón, Jesús Herrero, Ramón Agüero, Arancha Rodríguez, Santiago Albillos, Javier Sainz, Aránzazu Sanz, and David Gómez

Multi-hop Extensions to Heterogeneous Access Network Selection 43
Ramón Agüero, Johnny Choque, and Luis Muñoz

Experimental System Level Platform for B3G Scenarios 57
V. Monteiro, J. Bastos, O. Cabral, F. Velez, and J. Rodriguez

MobiLight 2010 – Special Session on "QoS Provision in Wireless Networks (QPWN)"

TCP-Aware Forward Error Correction for Wireless Networks 68
Dzmitry Kliazovich, Magda Bendazzoli, and Fabrizio Granelli

Delay Performance Analysis of a Two-Stage Cross-Layer Scheduler for Wireless LANs 78
Andreas Könsgen and Carmelita Görg

Access Network Selection in a Heterogeneous Environment Using the AHP and Fuzzy TOPSIS Methods 88
Aggeliki Sgora, Periklis Chatzimisios, and Dimitrios D. Vergados

Adaptive Message Ferry Route (aMFR) for Partitioned MANETs 99
Ting Wang and Chor Ping Low

Lightweight Mechanisms for Self-Configuring Protocols 112
Eleni Patouni and Nancy Alonistioti

Analysis of the Energy Consumption of JavaScript Based Mobile Web Applications 124
Antti P. Miettinen and Jukka K. Nurminen

MobiLight 2010 – Special Session on "Advanced Radio Access Techniques for Energy-Efficient Communications (MIMAX)"

Equal Gain MIMO Beamforming in the RF Domain for OFDM-WLAN Systems 136
Álvaro Gonzalo, Ignacio Santamaría, Javier Vía, Fouad Gholam, and Ralf Eickhoff

A Framework for the Design Space Exploration of Software-Defined Radio Applications 148
Thorsten Jungeblut, Ralf Dreesen, Mario Porrmann, Michael Thies, Ulrich Rückert, and Uwe Kastens

On the Maximum Efficiency of Power Amplifiers in OFDM Broadcast Systems with Envelope Following 160
Robert Wolf, Frank Ellinger, and Ralf Eickhoff

Equal-Phase Beamforming Architecture for RF-MIMO Antenna Systems 171
Fouad Gholam, Javier Vía, Alfredo Nazábal, and Ignacio Santamaría

Optimal Channel and Power Allocation for Secondary Users in Cooperative Cognitive Radio Networks (Invited Paper) 180
Mario Bkassiny and Sudharman K. Jayaweera

MobiLight 2010 – Special Session on "Security and Resilience in the Future Internet (SECURE)"

User Authentication Method and Implementation Using a Three-Axis Accelerometer 192
Alexandros Zaharis, Adamantini Martini, Panayotis Kikiras, and George Stamoulis

A Correlation Approach to Intrusion Detection 203
Massimo Ficco and Luigi Romano

A Dynamic Key Agreement Mechanism for Mission Critical Mobile Ad Hoc Networking 216
Ioannis G. Askoxylakis, Theo Tryfonas, John May, and Apostolos Traganitis

Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks 229
Giacomo de Meulenaer and François-Xavier Standaert

Sensor Networks – Critical Infrastructure for Society? Challenges for Resilience, Security and Interoperability 243
Alistair Munro

Wide–Weak Privacy–Preserving RFID Authentication Protocols 254
Yong Ki Lee, Lejla Batina, Dave Singelée, and Ingrid Verbauwhede

A Preliminary Study of a Wireless Process Control Network Using Emulation Testbeds 268
Michele Guglielmi, Igor Nai, Andres Perez-Garcia, and Christos Siaterlis

MobiLight 2010 – Special Session on "Self-Management in Future Internet Wireless Networks (SELFNET)"

CogProt: A Framework for Cognitive Configuration and Optimization of Communication Protocols 280
Dzmitry Kliazovich, Neumar Malheiros, Nelson L.S. da Fonseca, Fabrizio Granelli, and Edmundo Madeira

Topology Control in Self-managed Wireless Networks 292
Apostolos Kousaridas and Nancy Alonistioti

Autonomicity and Self-manageability Techniques in the Scope of the Future Internet's Evolution 302
Ioannis P. Chochliouros, Anastasia S. Spiliopoulou, Maria Belesioti, Evangelos Sfakianakis, George Diakonikolaou, Andreas Rigas, Evangelia Georgiadou, George Agapiou, and Tilemachos Doukoglou

Design and Development of Essential Use-Cases for Self-management in Future Internet Wireless Networks 318
Ioannis P. Chochliouros, Evangelos Sfakianakis, Apostolis Kousaridas, Jens Modeker, David Wagner, Anastasia S. Spiliopoulou, George Agapiou, Andrej Mihailovic, Dev Pramil Audsin, Maria Belesioti, Andreas Rigas, Konstantinos Chelidonis, Evangelos Gazis, Gerard Nguengang, Nancy Alonistioti, Christos Mizikakis, Dimitrios Katsaros, and Tilemachos Doukoglou

Towards Dynamic Protocol Configuration and its Configuration and Control in Autonomous Communication Environments 334
David Wagner and Jens Mödeker

MobiLight 2010 – Special Session on "Distributed Wireless Networking Experimental Infrastructure for Optimization and Convergence (ICARUS)"

Dynamic Call Admission Control for Enhanced GoS of UGS Connections during "Busy Hour" in WiMAX 346
Angelos Antonopoulos and Christos Verikoukis

Mutual Information Effective SNR Mapping Algorithm for Fast Link Adaptation Model in 802.16e 356
Fernando López Aguilar, Gorka Rubio Cidre, José Manuel López López, and Javier Regidor Paris

Virtual Distributed Simulation Platform for the Study and Optimization of Future Beyond 3G Heterogeneous Systems 368
M^a Carmen Lucas-Estañ, Salva Garrigas, Javier Gozálvez, Jose Monserrat, Julen Maneros, Fernando López, Ainara González, Imanol Aguado, and Pedro Chaparro

A Dual Head Clustering Mechanism for Energy Efficient WSNs 380
Muhammad Alam and Jonathan Rodriguez

Measuring the Closed-Loop Throughput of 2x2 HSDPA over TX Power and TX Antenna Spacing 388
Sebastian Caban, José A. García-Naya, Christian Mehlführer, Luis Castedo, and Markus Rupp

MobiLight 2010 – Special Session on "Critical Information Infrastructure Protection: Where We Stand and Where We Are Heading To (CIIP)"

Towards Benchmarking of P2P Technologies from a SCADA Systems Protection Perspective 400
Abdelmajid Khelil, Sebastian Jeckel, Daniel Germanus, and Neeraj Suri

Improving Wireless Sensor Network Resilience with the INTERSECTION Framework 415
Gareth Tyson, Adam T. Lindsay, Steven Simpson, and David Hutchison

Trust Management in Monitoring Financial Critical Information Infrastructures 427
Giorgia Lodi, Roberto Baldoni, Hisain Elshaafi, Barry P. Mulcahy, György Csertán, and László Gönczy

Using MPLS in a Wireless Mesh Network to Improve the Resiliency of SCADA Systems 440
Stefano Avallone and Salvatore D'Antonio

Fusion of Bayesian and Ontology Approach Applied to Decision Support System for Critical Infrastructures Protection 451
Rafał Kozik, Michał Choraś, and Witold Hołubowicz

MobiLight 2010 – Special Session on "Advanced Wireless Technologies for a Converged Ultra-Broadband Home Network (OMEGA)"

OMEGA: New Use Cases for Future Home Networks 464
Jean-Philippe Javaudin, Martial Bellec, Gilles Goni, and Rafael Gonzalez Fuentetaja

Adaptive Filter Bank Modulation for Next Generation Wireless In-Home Networks 472
Salvatore D'Alessandro and Andrea M. Tonello

Challenges in Gbps Wireless Optical Transmission 484
Mike Wolf, Jianhui Li, Liane Grobe, Dominic O'Brien, Hoa Le Minh, and Olivier Bouchet

An Efficient Power Control Algorithm for Supporting Cognitive Communications in Shared Spectrum Areas 496
Mahdi Pirmoradian, Christos Politis, and Emmanouil A. Panaousis

MobiLight 2010 – Special Sessions on "Advances on Indoor Positioning and Multiuser Scheduling (NEWCOM++)" and "Relay-Based Next Generation Wireless Broadband Networks and Associated Components (REWIND)"

TOA Estimation in UWB: Comparison between Time and Frequency Domain Processing 506
Eva Lagunas, Lorenzo Taponecco, Montse Nájar, and Antonio D'Amico

Trade-off between Feedback Load for the Channel State Information and System Performance in MIMO Communications 518
Daniel Sacristán-Murga and Antonio Pascual-Iserte

Evolution of Spatial and Multicarrier Scheduling: Towards Multi-cell Scenario 530
Pol Henarejos, Ana Perez-Neira, Velio Tralli, Marco Moretti, Nikos Dimitriou, and Giulio Dainelli

Multi-hop Relay in Next Generation Wireless Broadband Access Networks: An Overview 543
Nikos Athanasopoulos, Panagiotis Tsiakas, Konstantinos Voudouris, Iraklis Georgas, and George Agapiou

EUMOBILE 2010 – 1st European Symposium on “Mobility Management”

An Experimental MIH Platform for Testing Video Streaming Services across Heterogeneous Radio Access Technology Networks 555
Lampros Dounis, Michail Tsagaropoulos, Ilias Politis, and Tasos Dagiuklas

A Lightweight Macro-Mobility Framework 567
Karel De Vogeleer, David Erman, Markus Fiedler, and Adrian Popescu

Enhanced Localization in Wireless Ad Hoc Networks through Cooperation 579
Senka Hadzic, Joaquim Bastos, and Jonathan Rodriguez

Increasing the VoIP Capacity through MAP Overhead Reduction in the IEEE 802.16 OFDMa Systems 590
Vitaliy Tykhomyrov

Multi-radio Cooperative ARQ in Wireless Cellular Networks: A MAC Layer Perspective 604
J. Alonso-Zárate, E. Kartsakli, L. Alonso, M. Katz, and Ch. Verikoukis

PHYLOM 2010 – Workshop on “Advanced PhYsical Layer Optimization Methods for Energy-Efficient Wireless Systems”

Joint Turbo Coding and Source-Controlled Modulation of Cycle-Stationary Sourcesin the Bandwidth-Limited Regime 618
Idoia Ochoa, Pedro M. Crespo, Javier Del Ser, and Mikel Hernaez

Harmony Search Heuristics for Quasi-asynchronous CDMA Detection with M-PAM Signalling 626
S. Gil-Lopez, J. Del Ser, and L. Garcia-Padrones

Cross-Layer Clustering Optimization in Mobile Networks Using Evolutionary Algorithms 638
L. Carro-Calvo, S. Maldonado-Bascon, A. Portilla-Figueras, S. Lafuente-Arroyo, and S. Salcedo-Sanz

A Case Study of Parameter Control in a Genetic Algorithm: Computer Network Performance 650
J.A. Fernández-Prieto, J. Canada-Bago, M.A. Gadeo-Martos, and Juan R. Velasco

On the Application of a Novel Grouping Harmony Search Algorithm to the Switch Location Problem 662
Sergio Gil-Lopez, Javier Del Ser, Itziar Landa, Laura Garcia-Padrones, Sancho Salcedo-Sanz, and Jose A. Portilla-Figueras

Adaptive Weighted Round Robin (AWRR) Scheduling for Optimization of the Wireless Medium Virtualisation 673
Gorka Hernando, Susana Pérez, and José María Cabero

Robust Wireless Network Coding – An Overview 685
Marco Di Renzo, Lana Iwaza, Michel Kieffer, Pierre Duhamel, and Khaldoun Al Agha

UAS 2010 – Workshop on "User Adaptive Systems for Mobile Wireless Systems"

Localization in Real GSM Network with Fingerprinting Utilization 699
Jozef Benikovsky, Peter Brida, and Juraj Machaj

Customized Contents Service Over a DVB-SH/3G Network 710
Azza Jedidi and Frédéric Weis

Measurement and Visualization of ECG on Mobile Monitoring Stations of Biotelemetric User Adaptive System 722
Dalibor Janckulik, Leona Motalova, and Ondrej Krejcar

Complex Mobile User Adaptive System Framework for Mobile Wireless Devices 739
Ondrej Krejcar

The Indoor Orientation of Autonomous Mobile Devices for Increasing Human Perspective 755
Jiri Kotzian, Jaromir Konecny, Ondrej Krejcar, Tomas Lippa, Hynek Prokop, and Marian Kuruc

Architecture and Design of Mobile Telemetry System for Ambient Assisted Living 769
Martin Stankus, Marek Penhaker, Jan Kijonka, Petr Grygarek, and Jiri Kotzian

Author Index 781

Performance of MC-DS-CDMA System in Rayleigh Fading Channel with Non-coherent Combining Schemes and MAI Interference

Ismahene Ikhlef[1], Abdellatif Said[2], Faouzi Soltani[1], and Faouzi Bader[3]

[1] University of Constantine,(UoC), Faculty of Engineering, Department of Electronics,
25000-Constantine, Algeria
[2] United Arab Emirates (UAE) University, UGRU- Math/IT,
PO Box 17172;Al Ain;Abu Dhabi;17172;UAE
[3] Centre Technologic de Telecomunicacions de Catalunya-CTTC,
PMT, av. Canal Olimpic s/n, 08860-Barcelona
`r_messas@yahoo.fr,abdellatifs@uaeu.ac.ae`

Abstract. In this paper, we analyzed the multi – carrier direct sequence code division multiple access system when the received signal is divided into predetermined spreading sequences, and the sub - bands are modulated over *M* carriers. Because of the unknown phase of the received signal at each sub-band the receiver cannot coherently combine the outputs of the correlators. We consider in this paper non-coherent combining scheme (equal gain combining) with MAI interferences. The calculation of the probabilities of detection and false alarm for both multicarrier (MC) and single carrier (SC) system in a Rayleigh fading channel demonstrated that the performances of the multicarrier system are better than those with single carrier system. Obtained results demonstrated that the suppression (or the mitigation) of appeared interferences is obtained by the increase of the number of system carriers[1].

Keywords: CDMA, multi-carrier DS-CDMA, equal gain combining, non-coherent combing scheme.

1 Introduction

The problem of allowing multiple users to simultaneously access a channel without causing an undue amount of degradation in the performance of any individual user is a classical problem in communication systems.

The two most common access techniques are; the frequency division multiple access (FDMA), and the time division multiple access (TDMA), which attempt to solve the problem by spreading the signal in frequency and time respectively.

For instance, in the FDMA access scheme the inter-modulation problem will be the most generated difficulty. However, In the TDMA access scheme the inter-modulation

---

[1] This work has been partially carried out in the framework of the European Celtic project MOBILIA (CP5-016), and in the Spanish National project TSI-020400-2008-82, and partially supported by the project PHYDYAS/FP7-ICT-2007-1-211887

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 1–10, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

problem does not exist, but an accurate synchronization of all the users becomes of paramount importance during the system design.

Furthermore, whether an interference or multipath effect is present (which will be the case in this proposal), degradation in system performance can result in either FDMA or TDMA [1] multiple access schemes. The code division multiple access (CDMA) system seems more suitable in such adverse environments as it offers more robustness against the effects of the multi-user interference degradation. For that reason the CDMA is still considered as a potential candidate for future generation communications system. [1].

In this proposal the authors propose a multi-carrier direct sequence (MC-DS) CDMA system transmitting over a Rayleigh fading channel. The MC-DS-CDMA system has free interference capability which could be achieved among other techniques by correlating the received signal with predetermined spreading sequences. Thus allowing that the inherent processing gain of the system attenuating the interference effects [2], [3]. For that, the use of a chip waveform filter is necessary to reject the narrow band and/or the self interferences.

The serial acquisition performance of a MC-DS-CDMA system has been widely investigated in [4], where each subcarrier signal is subject to frequency-selective fading. The performance of the parallel code acquisition of a MC-DS-CDMA system has been analyzed in [5] for the case where each subcarrier signal is subject to a frequency-non-selective, and modeled as fading or non-fading (with or without partial band interference by computing the probability of error).

In this work, we consider the MC-DS-CDMA system and we study the probabilities of detection and false alarm, we also consider the single carrier SC-CDMA systems in presence of additive white Gaussian noise (AWGN) and multiple access interference (MAI) transmitting over a Rayleigh fading channel with equal gain combining (EGC) equalization. This paper is organized as follows: Section 2 introduces the system model for the proposed multicarrier DS-CDMA system. The statistics of the outputs of the non-coherent correlators and combiners for Rayleigh fading channel are presented in section 3 and 4, as well as the calculation of the probability of detection and false alarm. In section 5, we compared the numerical results for both multicarrier and single carrier CDMA systems using the proposed equal gain combining. Finally, we provide our conclusions in section 6.

2 System Description

2.1 Transmitter

The block chain of the *k-th* active user's transmitter using CDMA scheme is depicted in Figure 1, where the data $d\left(\frac{n}{N_D}\right)^{(k)}$ is generated as a random binary sequence, where $c_n^{(k)}$ is a pseudo – random (also named as Pseudo Noise-PN) spreading signature sequence with $n=\{1,...N_D\}$, N_D means the spreading gain. We assume that each signature has N_D chips of duration T_c per symbol which represent also the spreading gain code; the $d\left(\frac{n}{N_D}\right)^{(k)} c_n^{(k)}$ sequence is modulated by an impulse train with energy per chips equal to E_c. The transmitted signal at the output of the chip wave – shaping filter modulates M subcarriers. The energy per-chip of the modulating signal over each carrier is $\frac{E_c}{M}$. Finally, the spectral spreading is imposed on the complex signal by multiplying it with a spreading code. Therefore, the transmitted signal of the k-th user [5]- [6]-[7] has the following expression

$$S_k(t)=\sqrt{\frac{2E_c}{M}}\sum_{n=-\infty}^{+\infty} d_{\left(n/N_D\right)}{}^{(k)}c_n{}^{(k)}h(t-nMT_c)\sum_{m=1}^{M}\cos(\omega_m t+\theta_{k,m}) \tag{1}$$

Where *h(t)* means the impulse response of the chip wave- shaping filter, and $\theta_{k,m}$ is a random phase uniformly distributed over [0, 2π] range. In MC-DS-CDMA systems the modulated subcarriers are orthogonal over the chip duration. Hence, the frequency corresponding to the m-th subcarrier is $f_m = f_p + m/T_c$, where f_p is the fundamental carrier frequency.

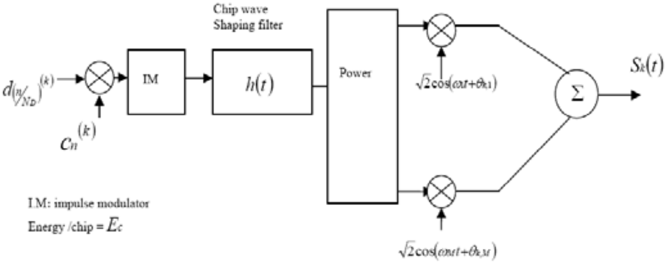


Fig. 1. The schematic blocs of the MC-DS-CDMA transmitter

2.2 The Channel

The assumed channel is a slowly varying frequency selective Rayleigh channel with a transfer function of the frequency band of the *k-th* user equal to $\alpha_{k,m}\exp(j\beta_{k,m})$, where $\alpha_{k,m}$ and $\beta_{k,m}$ are independent and identically distributed (i.i.d) Rayleigh random variables with a unit second moment, and uniform random variables over [0, 2π] respectively. Consequently, the received signal can be written as [5]:

$$r(t)=\sum_{k=1}^{K}\sqrt{\frac{2E_c}{M}}\left\{\sum_{n=-\infty}^{+\infty} d_{(n+D_k)/N_D}{}^{(k)}c_{(n+D_k)}{}^{(k)}h(t-nMT_c-\zeta_k)\right.$$
$$\left.\sum_{m=1}^{M}\alpha_{k,m}\cos(\omega_m t+\theta'_{k,m})\right\}+n_w(t) \tag{2}$$

We suppose in our proposal free partial band interference (PBI), $n_w(t)$ means the additive white Gaussian noise (AWGN) with a double side power spectral density (PSD) of $\eta_0/2$ and $\theta'_{k,m}=\theta_{k,m}+\beta_{k,m}$ is uniformly distributed over [0,2π], D_k is the code chip phase sequence of the *k-th* user, ζ_k means the unknown offset time defined as $\zeta_k = D_k M T_c + \tau_k$. Here τ_k is the unknown chip delay assumed to be uniformly distributed over $[0, MT_c]$.

2.3 The Receiver

The block diagram of the receiver of the k-th user is shown in both; Figure 2 and, where there is an in-phase (I) and quadratic (Q) correlators for each one of the M subcarriers. Each one of the in-phase and quadratic non-coherent correlator is composed by a coherent demodulator and a low pass filter (LPF) such that each double frequency terms can be ignored [5] (see Figure 2). The outputs of the low pass filter are sampled and despreaded by a local PN code replica. After the correlation process, the output is squared by a quadratic envelope detector and their outputs are summed in both branches; I and Q. The signal summation results passes through an adaptive gain amplifier for each of the M non-coherent correlators to produce the decision component within the symbol combiner (see Figure 3). The authors propose to handle the acquisition process by means of a sequential method where the incoming signal is correlated serially with all the possible phases of the local PN code replica. The result of this operation is stored within the symbol combiner. We assume that the chip wave-shaping filter has the following characteristics: $X(f) \equiv |H(f)|^2$ satisfied, the Nyquist criterion, $\int_{-\infty}^{+\infty} X(f) \equiv 1$, and $X(f)$ is band limited to whole W' system bandwidth such that $W' \leq \frac{f_{m+1} - f_m}{2}$. These imply that the direct spread waveform does not overlap the adjacent bands and therefore we have free adjacent channel interferences (CI) [5]. To ensure the above filter characteristics, $X(f)$ (see Figure 3) is a raised-cosine filter with the characteristic shown in (3) [8]-[9].

$$X(f) = \begin{cases} \frac{1}{W'} & |f| \leq \frac{W'}{2}(1-\alpha) \\ \frac{1}{2W'}\left\{1 - \sin\left[\frac{1}{2\alpha}\left(\frac{2\pi |f|}{W'} - \pi\right)\right]\right\} & \frac{W'}{2}(1-\alpha) \leq |f| \leq \frac{W'}{2}(1+\alpha) \\ 0 \quad elsewhere & \end{cases} \tag{3}$$

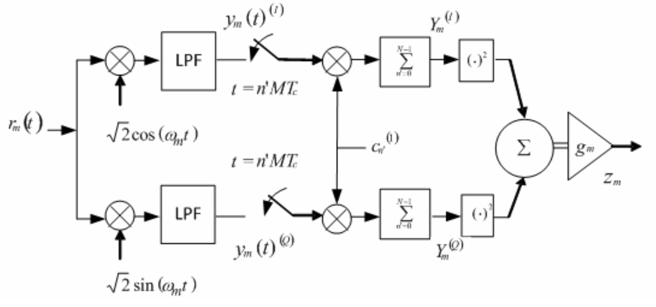


Fig. 2. The non-coherent correlator (I,Q) for the each *m-th* subcarrier

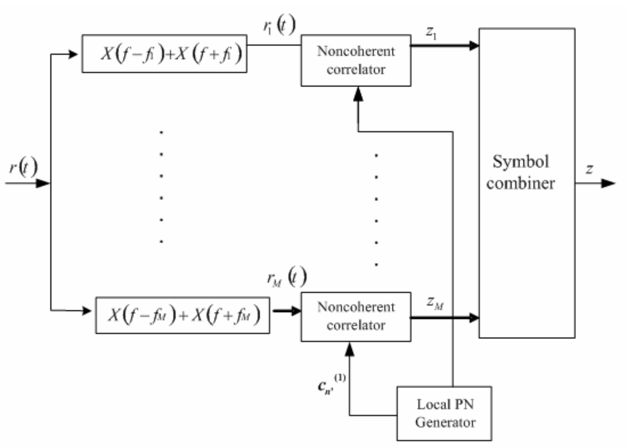


Fig. 3. The receiver of the multi-carrier DS – CDMA system

3 The Statistics of the Outputs of the Non-coherent Correlator and Combiner

3.1 The Statistics of the Non-coherent Correlator

We assume that during the acquisition process no data are transmitted i.e. $d_{(n+D_1)/N_D}^{(1)}=1$, and the outputs of the non-coherent correlator of the m-th branch are given by

$$z_m = g_m^{-1}\left\{ \left(Y_m^{(I)}\right)^2 + \left(Y_m^{(Q)}\right)^2 \right\} \tag{4}$$

Where g_m^{-1} represent the adaptive gain control (AGC) over the m-th branch assumed perfectly estimated from the average received power and is given by:

$$g_m = \overline{y_m^{(I)}(n'MT_c)^2 + y_m^{(Q)}(n'MT_c)^2} \tag{5}$$

Where $\overline{(.)}$, means the average calculation. The terms $\overline{y_m^{(I)}(n'MT_c)^2}$ and $\overline{y_m^{(Q)}(n'MT_c)^2}$ are; the in phase and the quadratic sampled signals at rate ($n'MT$) respectively (see) and are equal to:

$$y_m^{(I)} = \alpha_{1,m} S(\zeta_1)\cos(\theta'_{1,m}) + I_{y_m}^{(I)} + N_{y_m}^{(I)}$$

$$y_m^{(Q)} = \alpha_{1,m} S(\zeta_1)\sin(\theta'_{1,m}) + I_{y_m}^{(Q)} + N_{y_m}^{(Q)} \tag{6}$$

Where $S(\zeta_1) = \sqrt{E_c/M} \sum_{n'=0}^{N-1} \sum_{n=-\infty}^{+\infty} c_{n'}^{(1)} c_{n+D_1}\, x[(n'-n)MT_c - \zeta_1]$ represent the desired detected signal, $I_{y_m}^{(I)}$ and $I_{y_m}^{(Q)}$ are the interference parts in each of the in phase and quadratic branches respectively. And similar to the interference parts, we have $N_{y_m}^{(I)}$ and $N_{y_m}^{(Q)}$ which are the experienced noise in the in-phase and the quadratic signals respectively. For the Rayleigh fading channel, the conditional probability density function (p.d.f) on H_i (i=0,1) of z_m is given by [5]:

$$p\left(z_m / H_i \right) = \frac{1}{2v'_{m,i}} \exp\left(-\frac{z_m}{2v'_{m,i}} \right)$$
$$where \quad v'_{m,i} = v_{m,i} + \frac{m'^{\,2}_{m,i}}{2} \tag{7}$$

3.2 The Outputs of the Non-coherent Combiner

In this paper, we consider one kind of the non-coherent combiner scheme.

3.2.1 Equal Gain Combining (EGC)

In this kind of the symbol combining the output is given by [5]-[10]:

$$z = \sum_{m=1}^{M} z_m \tag{8}$$

For Rayleigh fading channel the characteristic function conditioned on H_i of z in (8) is the product of the all characteristics functions of z_m and is given by:

$$\Psi_{\left(z/H_1 \right)}(s) = \prod_{m=1}^{M} \Psi_{\left(z_m/H_i \right)}(s) \tag{9}$$

Where $\Psi_{\left(z_m/H_i \right)}(s)$ is the Fourier transform of the probability density function (p.d.f) of z_m which is obtained from (7). For a Rayleigh fading channel the characteristic function is expressed as

$$\psi_{\left(z_m/H_i \right)}(s) = \frac{1}{1 - 2v'_{m,i}\, s} \tag{10}$$

The probability density function of z is the inverse Fourier transform of its characteristic function from Cauchy residue theorem; we obtain the p.d.f. function as

$$p\left(z/H_i\right)=\frac{z^{M-1}\exp\left(-\frac{z}{2v'_{m,i}}\right)}{\left(2v'_{m,i}\right)^{M}Fact\left(M-1\right)} \tag{11}$$

The value $2v'_{m,i}$ is hereafter defined.

4 Calculation of the Probability of Detection and False Alarm

4.1 Probability of Detection

The probability of detection P_{Dfe} is provided by the integration of the probability density function of z in (11) over the normalized threshold γ^* ($\gamma^*=\gamma/N$) and the correlation period N [11]. Therefore we obtain the final expression of the probability of detection as

$$p_{Dfe}=\sum_{m=0}^{M-1}\left(\frac{\gamma^*}{(B+a)}\right)^{m}\frac{\exp\left(\frac{\gamma*}{(B+a)}\right)}{Fact(m)} \tag{12}$$

With $2v'_{m;i}=N\left(B+a\right)$, where B and a are calculated as the following

$$B=\frac{\left(1+(K-1)\,v\,\left(1-\alpha/4\right)\right)}{\left(1+K\,v\left(1-\alpha/4\right)\right)}$$

$$a=\frac{N\,v}{\left(1+K\,v\left(1-\alpha/4\right)\right)}$$

$$v=\frac{E_{c1}}{\eta_0}\ with\ E_{c1}=\frac{E_c}{M}$$

Where α means here the roll-off factor.

4.2 Probability of False Alarm

In a similar manner of calculation of p_{Dfe}, we can obtain the false alarm probability p_{Fafe} as:

$$p_{Fafe}=\sum_{m=0}^{M-1}\left(\gamma^*\right)^{m}\frac{\exp\left(\gamma^*\right)}{Fact(m)} \tag{13}$$

$$with\ \ v'_{m,0}=v_{m,0}+\frac{m'^{\,2}_{m,0}}{2}$$

5 Numerical Results

In this section, we make a comparison between the probability of detection and false alarm in Rayleigh Fading channel with no- partial band interference for both multi-carrier and single-carrier systems. The period of correlation of the single carrier has been chosen equal to $N_1=512$, but for the multi-carrier $N= N_1 /M$, and a roll-off factor α of the raised-cosine filter equal to 0.5 [5]-[8]-[9].

The expression of the probability of detection and false alarm contain too many parameters. Simulation results are obtained by MATLAB software, and by applying linear interpolation over the different points.

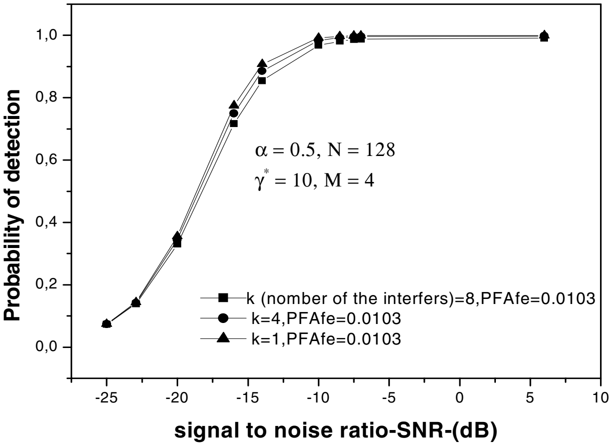


Fig. 2. Probability of detection for Rayleigh fading channel for a multi-carrier system (M≥2), with equal gain combining and using different values of *K*.

The significant inconvenient of the CDMA scheme is the multiple access interference (MAI). The effect of the MAI on both probabilities; of detection and false alarm using equal gain combining is shown in

Figure 2. It can be observed that when the number of interferes (undesirable users) increases, the probability of detection decreases. However the probability of false alarm remains constant, this could be explained by the fact that this probability doesn't depend on the value of *K* (active users).

In Figure 5, we can easily see that the minimization of the MAI interference is given by the increasing of the number of the carriers *M* which allows a very good probability of detection and a constant probability of false alarm. The performance of the multi-carrier system (for M=2,4) is better than the performance of the single carrier system (for M=1) because the probability of detection of the first system is greater than the probability of detection of the second system with a low probability of false alarm. Finally, in order to minimize the MAI interference, the use of the equal gain combining in MC-DS-CDMA is more than recommended.

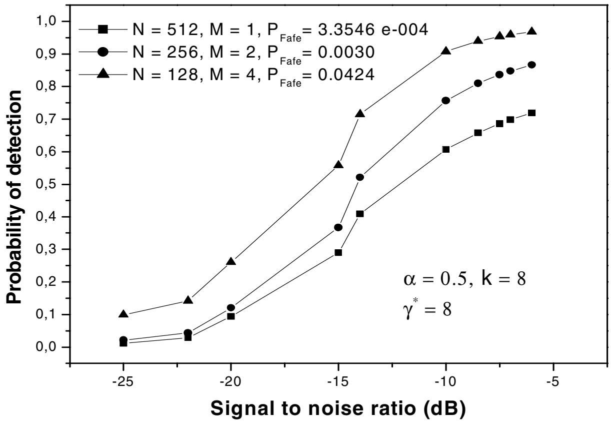


Fig. 3. Probability of detection for Rayleigh Fading channel for both multi-carrier (($M \geq 2$)) and single carrier (M=1) systems with the equal gain combining for different values of M, and number of interferes (K=8)

6 Conclusions

In this paper, we have analyzed the type of combination having an equal gain combining equalization in multicarrier and single carrier systems over a Rayleigh fading channel. We know that interferes (the undesirable users) represent the MAI interference; the results demonstrate that the increase of M minimizes this kind of interference. In the Rayleigh Fading channel, the performance of the multi-carrier system is better than the single carrier system for the equal gain combining.

Based on the obtained results, we recommend the use of the proposed equal gain combiner for multi-carrier CDMA system in the Rayleigh fading channel, especially when the MAI exists in order to minimize it. The increase of the number of subcarrier helps such mitigation.

References

1. Cook, C.E., Ellersick, F.W., Milstein, L.B., Schilling, D.L.: Spread-Spectrum Communications. IEEE Press, Inc., New York (copyright 1983)
2. Rowitch, D.N., Milstein, L.B.: Convolutional coded multicarrier DS-CDMA in-a multipath channel-part I. IEEE Trans. Commun. 47(10), 1570–1582 (1999)
3. Pickholtz, R.L., Schilling, D.L., Milstein, L.B.: Theory of spread spectrum communications-A tutorial. IEEE Trans. Commun. COM-30(5) (May 1982)
4. Yang, L.L., Hanzo, L.: Serial acquisition performance of single-carrier and multicarrier DS-CDMA over Nakagami-m Fading channels. IEEE. Trans. on Commun. 1(4), 692–702 (2002)
5. Lee, D., Milstein, L.B., Lee, H.: Analysis of multicarrier DS-CDMA code–acquisition system. IEEE Trans. Commun. 47(8), 1233–1243 (1999)

6. Kondo, S., Milstein, L.B.: On the performance of multicarrier DS-CDMA systems. IEEE Trans. Commun. 44, 238–246 (1996)
7. Bingham, J.: Multicarrier modulation for data transmission: An idea whorse time has come. IEEE Commun. Mag. (May 1990)
8. Wong, T.F., Lok, T.M., Lehnert, J.S.: Asynchronous multiple-access interference suppression and chip waveform selection with aperiodic random sequences. IEEE Trans. Commun. 47(1), 103–114 (1999)
9. Nguyen, H.H.: Effect of chip waveform shaping on the performance of multicarrier CDMA systems. IEEE Transactions on vehicular technology 54(3), 1022–1029 (2005)
10. Coulon, F.: Theory and treatment of signals. Edition Georgi. Dunod, Paris (1984)
11. Viterbi, A.J.: CDMA principles of spread spectrum communication. Addison Wesley Longman, Inc., Amsterdam (copyright 1995)

Spectral Efficiency Using Combinations of Transmit Antenna Selection with Linear Dispersion Code Selection

I. Gutierrez[1] and F. Bader[2]

[1] Advanced Technology, Standards and Regulation (ATSR),
Samsung Electronics Research Institute (SERI), Communications house,
South Street, Staines, Middlesex TW18 4QE, London, UK
Tel.: +44 (0) 1784 428600
[2] Centre Tecnològic de Telecomunicacions de Catalunya-CTTC
PMT- Building B4. Av. Carl Friedrich Gauss 7, 08860 – Castelldefels, Barcelona, Spain
Tel.: +34 936452909; Fax: +34 936452901
i.gutierrez@samsung.com, faouzi.bader@cttc.es

Abstract. In this paper the objective is to enhance the spectral efficiency using combinations of transmit antenna selection with Linear Dispersion Code Selection. Both bit error rate minimization and throughput maximization criteria are here examined[1]. The performance of the proposed spatial link adaptation scheme is evaluated under low mobility environments concluding that in case of linear receivers the transmit antenna code selection scheme with the combination of adaptive modulation and coding achieves a noticeable SNR gain (up to 3dB) in a large SNR margin (SNR from 6 to 18dB), which could be considered as a potent technique to achieve a smooth transition between diversity and multiplexing in order to maximize the overall system throughput.

Keywords: WiMAX, Spatial time coding, Transmit Antenna Selection, Linear Dispersion Codes, spectral efficiency.

1 Introduction

The use of multiple antennas at the transmitter and at the receiver has demonstrated the benefits of increasing the channel capacity and diversity [1]. Multiple Input Multiple Output (MIMO) systems may exploit the channel diversity and capacity by using different space-time-(frequency) coding techniques. When the channel state information is available at the transmitter (CSIT), the best space time coding technique is the beamforming where the information is transmitted in the strongest eigenmode(s) of the channel and the power is allocated to each eigenmode following the water-filling principle. However, CSIT techniques require that the transmitter estimates the full channel matrix which in some scenarios might become unfeasible.

---

[1] This work has been partially carried out in the framework of the European Celtic project MOBILIA (CP5-016), and in the Spanish National project TSI-020400-2008-82, and also supported in part by the project PHYDYAS/FP7-ICT-2007-1-211887.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 11–21, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

On the other hand, if CSI is not available at the transmitter, the well known Space-Time Block Coding (STBC) schemes are preferred. Hassibi and Hochwald proposed in [2] a framework where any kind of linear STBC could be analyzed, classifying such class of space-time codes as Linear Dispersion Codes (LDC). The main advantage from the LDCs is that different tradeoffs between diversity and spatial multiplexing (SM) can be achieved thanks to proper design of the code [2] [3]. As a result, different authors have proposed to use LDCs, since specific LDC codes structures are able to optimize particular channel metrics or enhance certain parameters (i.e. channel capacity, outage probability, bit error rate, etc.) [4][5].

Nevertheless, many research efforts have been done in order to exploit the best from each approach under the concept of Partial CSIT (PCSIT). In this case, the transmitter is provided only with a small amount of information about the channel state (e.g. Frobenius channel norm, channel rank, channel [6] [7] condition number, etc.), thus the transmitter sets up the transmitted signal to the current channel (this is referred as precoding). The simplest scheme of precoding is the Transmit Antenna Selection (TAS) where the best (set of) antenna(s) are selected for transmission. Actually, it has been demonstrated that the TAS scheme gives the same diversity order than without antenna selection at the expense of reducing the coding gain [8]. This effect has been analyzed in [8]-[10] for Spatial Multiplexing, Orthogonal STBCs and LDCs respectively. Yet, another well-known precoding technique which fixes the set of precoding matrices from a limited codebook (known a priori from both transmitter and receiver) has also shown to provide large capacity and link reliability improvement by using a low rate channel feedback providing uniquely the codeword index [11] [12].

As a result, the latest researches have combined both types of precoding (TAS and codebook-based) schemes for further enhance of the system performance. This paper extends the works in [13] [14] by applying both the TAS and codebook-based precoding schemes from a pure LDC perspective. Then, a spatial adaptation scheme for the downlink/uplink is developed where the proper Transmit antenna subset and LDC (from a set of predefined LDCs) are selected for each frame. Two optimization criteria (i.e. minimizing the bit error rate and maximizing the throughput) are evaluated showing that both the diversity order and the system throughput are maximized. In this paper the proposed scheme is referred as the Transmit Antenna and Code Selection (TACS).

The rest of the paper is organized as follows. In Section 2, the system model considered and the LDC code structure is introduced. The proposed TACS space-time adaptations criteria are detailed in Section 3 and the corresponding simulation results are analyzed in Section 4. Finally, conclusions are stated in Section 5, where the main Performance behaviors of the proposed approaches are exposed.

2 System Model

The MIMO system model with M and N transmitter and receiver active antennas respectively is defined by

$$\mathbf{Y} = \sqrt{\frac{\rho}{M}}\mathbf{H}\mathbf{S} + \mathbf{N}, \tag{1}$$

where $\mathbf{S} \in \mathbb{C}^{M \times T}$ and $\mathbf{Y} \in \mathbb{C}^{N \times T}$ are the transmitted and the received signals from each antenna during each channel access, and the channel matrix $\mathbf{H} \in \mathbb{C}^{N \times M}$ is assumed constant during T periods (i.e. block fading channel model). The transmitted signal has unitary power, and the noise matrix $\mathbf{N}$ follows a circular complex Gaussian distribution with zero mean and unitary standard deviation. The Linear Dispersion Code (LDC) structure subsumes most of the previous Space-Time (ST) codes such as the Bell-Labs Layered Architecture Space Time coding (BLAST), the Alamouti scheme, etc. [2]. Then, considering the LDC framework, the transmitted signal matrix $\mathbf{X}$ has necessarily the following structure

$$\mathbf{S} = \sum_{q=1}^{Q} \left(\alpha_q \mathbf{A}_q + j\beta_q \mathbf{B}_q \right), \tag{2}$$

where $\mathbf{A}$, $\mathbf{B} \in \mathbb{C}^{M\times T}$ are the basis matrices, $\mathrm{E}\{\mathrm{tr}(\mathbf{S}^H\mathbf{S})\}=MT$, and the values $s_q = \alpha_q + j\beta_q$ are the complex data symbols we want to transmit with $\mathrm{E}\{s_q^* s_q\}=1$. The number of basis matrices is Q, and the spatial multiplexing rate is Q/MT. The rate R achieved by the system is given by $R=Qn/T$ [bits/s/Hz], where n means the number of bits transmitted per each complex symbol.

Then substituting (2) into (1) and applying the *vec* operator on both sides of the expression, the (real valued) system equation can be rewritten as

$$\underbrace{\begin{bmatrix} \Re(\mathbf{y}_0) \\ \Im(\mathbf{y}_0) \\ \vdots \\ \Re(\mathbf{y}_{Q-1}) \\ \Im(\mathbf{y}_{Q-1}) \end{bmatrix}}_{\triangleq \boldsymbol{y}} = \sqrt{\frac{\rho}{M}}\mathcal{H} \underbrace{\begin{bmatrix} \alpha_0 \\ \beta_0 \\ \vdots \\ \alpha_{Q-1} \\ \beta_{Q-1} \end{bmatrix}}_{\triangleq \boldsymbol{s}} + \underbrace{\begin{bmatrix} \mathbf{n}_0 \\ \mathbf{n}_0 \\ \vdots \\ \mathbf{n}_{Q-1} \\ \mathbf{n}_{Q-1} \end{bmatrix}}_{\triangleq \boldsymbol{n}} \tag{3}$$

where $\mathbf{s}$ is the real input symbols vector and $\mathbf{n}$ is the real vector noise i.i.d. components $\mathcal{N}(0,1/2)$-distributed. The equivalent real valued channel matrix $\mathcal{H} \in \mathbb{R}^{2NT\times 2Q}$ is then given by

$$\mathcal{H} = \underbrace{\left[\mathbf{I}_N \otimes \mathcal{A}_0 \quad \mathbf{I}_N \otimes \mathcal{B}_0 \quad \cdots \quad \mathbf{I}_N \otimes \mathcal{A}_{Q-1} \quad \mathbf{I}_N \otimes \mathcal{B}_{Q-1} \right]}_{2NT\times 4MNQ} \times \underbrace{\left[\mathbf{I}_{2Q} \otimes \underline{h} \right]}_{4MNQ\times 2Q}. \tag{4}$$

With

$$\mathcal{A}_q = \begin{bmatrix} \Re\{\mathbf{A}_q\} & -\Im\{\mathbf{A}_q\} \\ \Im\{\mathbf{A}_q\} & \Re\{\mathbf{A}_q\} \end{bmatrix}_{2T\times 2M}, \quad \mathcal{B}_q = \begin{bmatrix} -\Im\{\mathbf{B}_q\} & -\Re\{\mathbf{B}_q\} \\ \Re\{\mathbf{B}_q\} & -\Im\{\mathbf{B}_q\} \end{bmatrix}_{2T\times 2M}, \quad \underline{h} = \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{N-1} \end{bmatrix}_{2MN}, \; h_n = \begin{bmatrix} \Re\{\mathbf{h}_n\} \\ \Im\{\mathbf{h}_n\} \end{bmatrix}_{2M}, \tag{5}$$

where $\mathbf{h}_n$ is the n-th row of the MIMO channel matrix $\mathbf{H}$.

Typically, the Maximum Likelihood (ML) detection is assumed during the LDCs design. However, it is well-known that the complexity requirements derived from such decoding techniques is extremely high ($\Theta(2^{Qn})$), making ML unaffordable for high data rates R in real implementations. Furthermore, due to the linear relationship between input and output samples observed in (3), a linear detector is enough to recover the symbols. However, the performance of such linear decoder is far from that offered by the ML. Nevertheless, one important benefit from using a linear decoder is that an equivalent channel can be estimated for each symbol. Hence Adaptive Modulation and Coding (AMC) can be applied on a per symbol basis. In this paper, a linear decoder using a Minimum Mean Square Error (MMSE) equalizer is only considered for evaluation of the TACS scheme.

Then, using a linear MMSE receiver, the Effective Signal to Interference and Noise Ratio (ESINR) per each symbol q is given by

$$ESINR_q^{(MMSE)}(\mathbf{H}) = \frac{\rho}{M\left[\mathbf{H}^H\mathbf{H} + 2\rho^{-1}\mathbf{I}_{2Q}\right]_{q,q}^{-1}} - 1, \tag{6}$$

where $\mathbf{X}^{-1}_{q,q}$ refers to the *(q,q)* element from $\mathbf{X}^{-1}$, and ρ is the average Signal to Noise Ratio (SNR). Furthermore, if the mapping applied to the symbols follows a 2^n-QAM constellation, the average pair wise error probability per stream applying the Nearest Neighbor Union Bound can be obtained as follows

$$P_{e,q} \leq 1 - \left(1 - N_e(n) \cdot \mathrm{E}\left\{Q\left(\sqrt{ESINR_q(\mathbf{H})\frac{d_{\min}^2(n)}{2}}\right)\right\}\right) \tag{7}$$

where $Q(x)=0.5\times erfc(x/2^{1/2})$, d^2_{min} is the squared minimum distance between any two points of the constellation (assuming an unitary average transmission power), and N_e is the average number of nearest neighbors constellation points. For a 2^n-QAM modulation $d_{min}{}^2=6/(2^n -1)$ and $N_e = 4\times(1-2^{-n/2})$. In addition, in case all the symbols within the codeword apply the same modulation, the average pairwise error probability for the whole codeword is usually approximated by (assuming $P_e<10^{-2}$)

$$P_e \leq Q \cdot N_e(n) \cdot \mathrm{E}\left\{Q\left(\sqrt{ESINR_{\min}(\mathbf{H})\frac{d_{\min}^2(n)}{2}}\right)\right\}, \tag{8}$$

where $ESINR_{min}=min(ESINR_0,\ldots, ESINR_{Q-1})$ [13].

3 The TACS Space-Time Adaptation Criteria

Then, given the ESNR per stream in (6) and the average pair wise error probabilities in (7) and (8), two different optimization scenarios are studied where both the transmit antenna subset as well as the best LDC from a set of codes are selected (see Fig 1).

In the first scenario, we consider that the same modulation is applied to all the symbols and that the rate R is fixed. In that case, and since transmission power is fixed, we are interested in selecting the transmit antenna subset and LDC code that minimizes the error rate probability (i.e. the bit error rate – BER) while the modulation that is required by each LDC is adapted in order to achieve the cited rate R. In that case, since the Q-function is monotonically decreasing as a function of the input, the optimization problem can be defined as follows

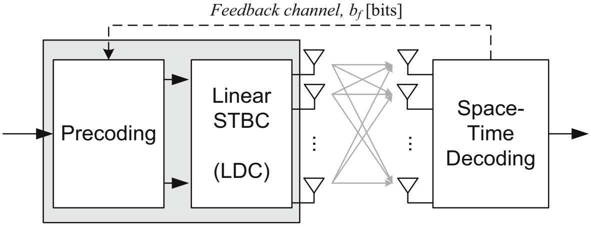


Fig. 1. TACS spatial adaptation scheme and its integration using adaptive LDC code selection

$$\max_{LDC_i, p_i} \min_{q} \left\{ ESINR_q \left(H, LDC_i, p_i \right) d_{\min}^2 \left(n_i \right) \right\}, \tag{9}$$

where i means the LDC index and p_i the transmitting antenna subset (set of antennas that can be used according to the number of transmitter antennas M_a and the number of antennas required by the LDC). It also noted that the constellation is a function of the LDC.

In the second scenario, the optimization is performed in order to maximize the system throughput considering a certain quality of service requirement (i.e. a maximum Block Error Rate - BLER). In that case, the problem is formulated as follows

$$\max_{LDC_i, p_i, MCS_j} \min_{q} R\left(1 - BLER\left(ESINR_q\right)\right) \quad \text{s.t.: } BLER \le \mu \tag{10}$$

where j means the Modulation and Coding Scheme (MCS) index that maximizes the spectral efficiency for the specific channel state subject to a maximum Block Error Rate (BLER). Actually, the selection of the optimum MCS is carried out assuming that the ESNR is the SNR that would be obtained at the receiver in case having an Additive White Gaussian Noise (AWGN) channel. Under that assumption, there is a direct mapping between each MCS and the obtained BLER for each ESNR.

4 Simulation Results

For the TACS evaluation, the downlink mode of a WiMAX TDD system has been used [15]. The number of available transmitter antennas are M_a={2,3,4} whereas the number of receiver antennas is fixed to N=2. One user is simulated which is allocated one subchannel per frame. The channel follows a spatial uncorrelated Rayleigh distribution whereas a block fading model is assumed per subchannel (flat in frequency and constant in time). It is assumed that the channel is perfectly known at both transmitter and receiver sides.

The performance of the TACS adaptation scheme in case the throughput is maximized (see Eq. (10)) is analyzed. Then, for such adaptation scheme, the antenna set and the LDC code that maximizes the throughput is selected. In addition, the highest MCS (in the sense of spectral efficiency) that achieves a BLER<0.01 (1%) is also selected. In these simulations the minimum allocable block length according the IEEE 802.16e standard was selected [15] (i.e. the number of subchannels N_{sch} occupied per block varies between 1 and 4). The number of available antennas is M_a=2 whereas N=2. Linear detection with the MMSE and ML detection are also compared.

The basic set of LDC codes that we have been used for the study are: the *Single Input Multiple Output* code using a Maximum Ratio Combiner (MRC), the *Alamouti* code (referred as G2 in the plots), the *BLAST*-like codes with M=2 (referred as Spatial Multiplexing, SM, in the plots) and the *Golden* code. The codeword length for all the codes is T=2. Moreover, for the SM case two types of encoding have been tested named vertical encoding (SM-VE) and horizontal encoding (SM-HE). For the vertical encoding, the same MCS is used for all the symbols transmitted within the same codeword, whereas for horizontal encoding each data stream (symbol) may apply a different MCS according to the channel status. Actually, all these codes are part of the standard and can be found in [15]. Consequently, since each i-th LDC from this basic set require at most two transmitting antennas, in case $M_i<M_a$ the best set p of transmitting antennas is selected from the M_a available antennas, and since the order in which the antennas are chosen is relevant we have P_i possible transmitting antennas combinations with

$$P_i = C\begin{pmatrix} M_a \\ M_i \end{pmatrix} = \frac{M_a!}{M_i!\left(M_a - M_i\right)!}. \tag{11}$$

To solve (9) or (10), an exhaustive search is performed among all the available LDC codes and P antenna sets, despite it would be very interesting testing the performance of the TACS under an incremental or decremental search as those proposed in [8].

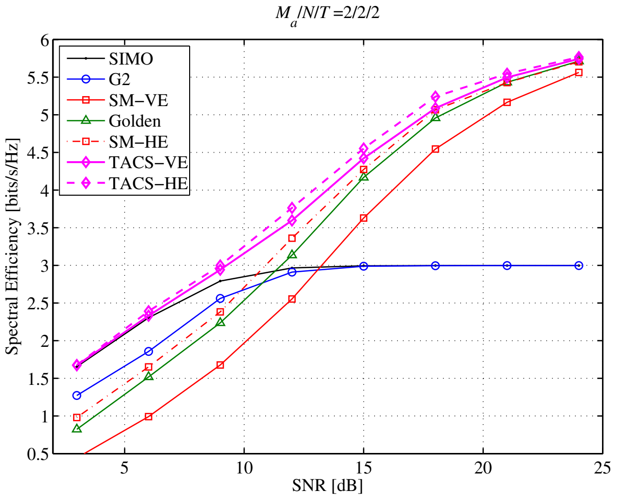


Fig. 2. Spectral efficiency achieved using the TACS scheme ($M_a/N/T$=2/2/2) joint with AMC under the throughput maximization criterion

The performance of TACS under the second optimization case and M_a=2 is shown in Fig 2. In this last scenario a PER bound of 1% is fixed and the MCS available are {4,16}-QAM with turbo-coding, with coding rates varying from 1/4 to 3/4. The MCS can be adapted on a per symbol (stream) basis. It is then shown that that at low SNRs (SNR<13dB) the SIMO and Alamouti achieved the highest spectral efficiencies.

However, as the SNR is increased, codes with higher multiplexing capacity are necessary; hence the SM and the Golden code achieve the highest spectral efficiencies. We also observed that the SM with VE implies a loss of around 2 dB compared to the Gold code, but when HE is used, the Gold code is around 0.5 dB worse than SM-HE. Above all, we observe that the TACS scheme with AMC gives the highest spectral efficiency where the highest benefit is obtained in the 8dB<SNR<18dB margin where a smooth transition between both types of codes (codes with g_s=1 or g_s=2) is carried out.

In case of MMSE receiver (Fig 3 and Fig 5), it is shown that at low SNRs (SNR<13dB) the SIMO and Alamouti schemes achieved the highest spectral efficiencies (something that has been already announced in several works [8]). However, as the SNR is increased the codes with higher multiplexing capacity (e.g. the SM and the Golden code) are preferred. We also observed that the SM with VE implies a loss of around 2dB compared to the Golden code, but when HE is used, the Golden code is around 0.5dB worse than the SM-HE.

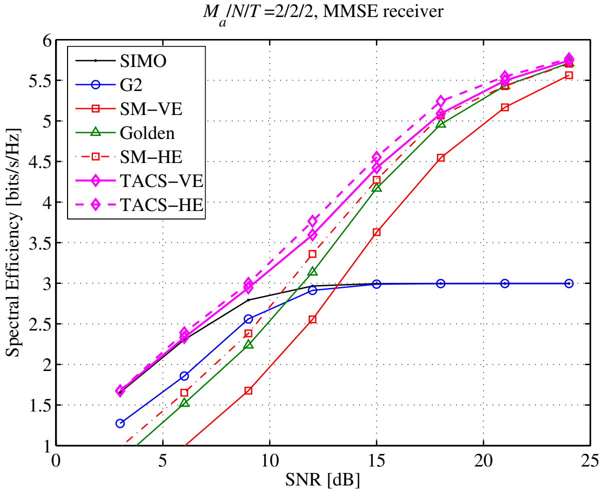


Fig. 3. Spectral efficiency under TACS with throughput maximization criterion with M_a=2, N=2, adaptive MCS and MMSE receiver for an uncorrelated MIMO Rayleigh channel

To gain further insights of the TACS behavior the statistics of LDC selection as a function of the average SNR are plotted in Fig 4. We can clearly appreciate that at low SNR the preferred scheme is SIMO where all the power is concentrated in the best antenna, while as the SNR is increased full rate codes (Q=M) are more selected since they permit to use lower size constellations. Moreover, comparing SM-VE with SM-HE, we can observe that SM-HE is able to exploit the stream's diversity and hence achieves a higher spectral efficiency than with the Golden code. Actually, at average SNR=12 dB, the SM with HE is the scheme selected for most frames, even more than SIMO.

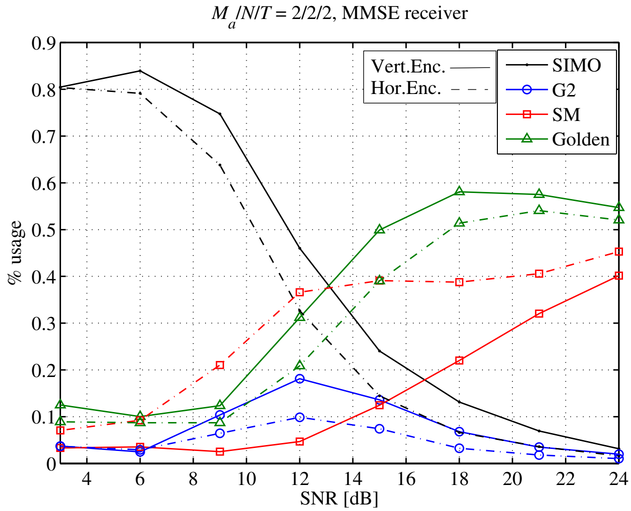


Fig. 4. LDC selection statistics under TACS with throughput maximization criterion with M_a=2, N=2, adaptive MCS and MMSE receiver for an uncorrelated MIMO Rayleigh channel

The evolution of the measured ESINR for the different streams is depicted in Fig 5 where the x-axis is scaled in channel accesses (i.e. time slots). It can be observed that SIMO is the scheme that achieves the highest ESINR values during the whole simulation time. Then few dBs below we have the Alamouti behavior, since it using both transmitter antennas the Frobenius channel norm dictates the ESINR evolution.

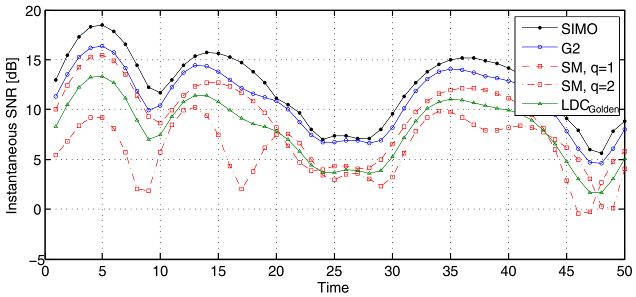


Fig. 5. Evolution of the ESINR per stream for different space-time codes with M_a=2, N=2, and time-correlated MIMO Rayleigh channel

Then, the ESINR achieved by different streams of the SM mode is plotted separately, where it can be seen that the best stream (SM_q, q=1) gets 3dB less than the ESINR using the SIMO scheme, this difference is due to the higher number of transmitter antennas that receive half the transmitting power. The second stream (SM_q, q=2) may fall several dB's (up to 10dB) compared to the best stream. This is the main reason why the SM-VE is so limited compared with the SM-HE. Finally, it is observed that the ESINR of the Golden code falls between the ESINR of both SM

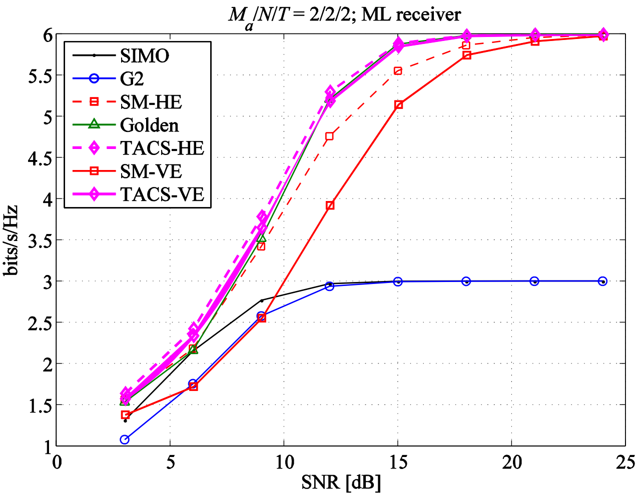


Fig. 6. Spectral efficiency under TACS with throughput maximization criterion with M_a=2, N=2, adaptive MCS and ML receiver for an uncorrelated MIMO Rayleigh channel

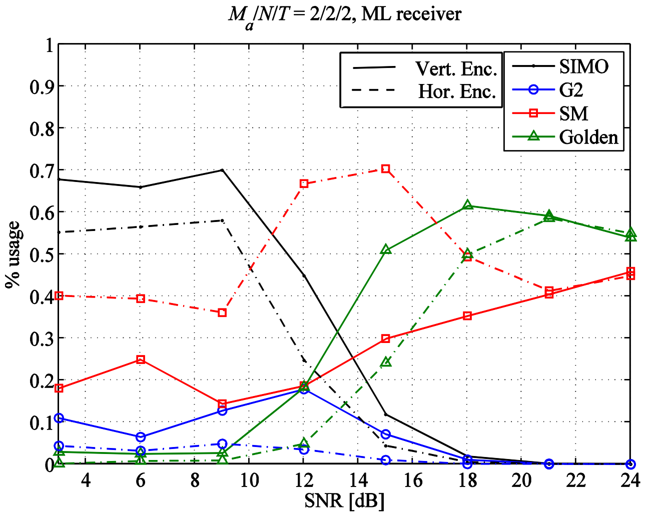


Fig. 7. LDC selection statistics under TACS with throughput maximization criterion with M_a=2, N=2, adaptive MCS and ML receiver for an uncorrelated MIMO Rayleigh channel

streams (q=1, q=2), however the Golden code's ESINR is lower than the arithmetic mean of the ESINR of both SM streams.

Next, the performance of the TACS with throughput optimization when using the ML decoder is shown in Fig 6 and Fig 7. Clearly, there is a large gain when using the ML compared to the previous MMSE detector. Something quite relevant is that when using the ML decoder, the Golden code achieves a capacity very close to that achieved by the TACS selection scheme (less than 1dB improvement due to the

TACS). This is a very logical result since the Golden code has been optimized assuming a ML decoder in order to maximize the capacity when *M=T=2* and the Z-QAM modulation which is the same case as analyzed during the simulations.

If we analyze the LDC selection statistics in Fig 7, similar results as in the MMSE case are obtained. It is observed that at low SNR values the SIMO looks like the preferred scheme, whereas at high SNRs both the Golden and the SM are chosen similarly (60% and 40% respectively). Furthermore, it is observed that at SNR range of 10dB to 18dB using the TACS scheme the SM-HE is the scheme selected most the time (even more than the Golden code). Again, the high spectral efficiencies achieved by the SM-HE in the above SNR range come from the fact that this code is able to exploit the diversity between streams when the AMC mode is applied.

5 Conclusions

As a conclusion, when using TACS with AMC and ML detection the benefits are not so clear even more if we take into account the signalling associated to the TACS scheme. Hence the focus in this case should be to use optimized LDCs codes for each {*M,T*} *pair*. However, obtained results shown that in case of linear receivers (e.g. MMSE) the TACS scheme with AMC achieves a noticeable SNR gain (up to 3dB) in a large SNR margin (SNR from 6 to 18dB), and also is a good technique to achieve a smooth transition between diversity and multiplexing. Then it seems also logical to consider the TACS scheme with linear receivers for the downlink where computational complexity at the mobile station must be kept as low as possible in order to save the batteries energy.

References

1. Telatar, E.: Capacity of multi-antenna Gaussian channels. European Transactions on Telecommunications (November 1999)
2. Hassibi, B., Hochwald, B.M.: High Rates Codes that are Linear in Space and Time. IEEE Communications Letters 5(4), 154–156 (2001)
3. Zheng, L., Tse, D.: Diversity and multiplexing: a fundamental tradeoff in multiple antenna channels. Proc. of the IEEE Trans. on Information Theory 49(5), 1073–1096 (2003)
4. Heath, R.W., Paulraj, A.J.: Linear Dispersion Codes for MIMO Systems Based in Frame Theory. Proc. of the IEEE Transactions on Signal Processing 50(10), 2429–2441 (2002)
5. Gohary, R., Davidson, T.: Design of Linear Dispersion Codes: Asymptotic Guidelines and Their Implementation. Proc. IEEE Transactions on Wireless Communications 4(6), 2892–2906 (2005)
6. Roh, J.C., Rao, B.D.: Multiple antenna channels with partial channel state information at the transmitter. Proc. IEEE Transactions on Wireless Communications 3(2), 677–688 (2004)
7. Love, D.J., Heath Jr., R.W., Santipach, W., Honig, M.L.: What is the value of limited feedback for MIMO channels? IEEE Communications Magazine 42(10), 54–59 (2004)
8. Oestges, C., Clerckx, B.: MIMO Wireless Communications. Academic Press, Elsevier, USA (2007)

9. Phan, K.T., Tellambura, C.: Capacity Analysis for Transmit Antenna Selection Using Orthogonal Space-Time Block Codes. IEEE Communications Letters 11(5), 423–425 (2007)
10. Deng, D., Zhao, M., Zhu, J.: Transmit Antenna Selection for Linear Dispersion Codes Based on Linear Receiver. In: Proc. IEEE Vehicular Technology Conference (IEEE VTC-Spring 2006) (2006)
11. Xia, P., Giannakis, G.B.: Design and Analysis of Transmit-Beamforming Based on Limited-rate Feedback. IEEE Transactions on Signal Processing 54(5), 1853–1863 (2006)
12. Love, D.J., Heath Jr., R.W.: Multimode precoding for MIMO wireless systems. IEEE Transactions on Signal Processing 53(10), 3674–3687 (2005)
13. Heath Jr., R.W., Love, D.J.: Multimode Antenna Selection for Spatial Multiplexing Systems with Linear Receivers. IEEE Transactions on Signal Processing 53(8), 3042–3056 (2005)
14. Sezgin, A., Jorswieck, E.A., Costa, E.: LDC in MIMO Ricean Channels: Optimal Transmit Strategy with MMSE Detection. IEEE Transactions on Signal Processing 56(1) (January 2008)
15. IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, IEEE Std. 802.16e^{TM}-2005 (February 2006)

A Reconfigurable Power Amplifier for Mobile WIMAX Applications

Yolanda Fernández, Miguel Angel Peña, and Francisco Díaz

TTI Telecommunication and Information Technologies,
Albert Einstein. 14, 39011 Santander, Spain
{yfernandez,mpena,fdiaz}@ttinorte.es

Abstract. This paper presents the design of a reconfigurable power amplifier for Mobile WIMAX applications in the user terminal. The amplifier, which operates from 3.4GHz to 3.5GHz, is based on the Doherty technique. This power efficiency enhancement technique is suitable for modern wireless communications systems, as Mobile WIMAX, that present with high peak-to-average power ratio (PAPR) to target high peak data rates while maintaining a trade-off between efficiency and linearity. In addition, reconfigurability in output power levels is added to the design to adapt it to different power scenarios. This work has been carried out in the framework of the CELTIC project MOBILIA, "Mobility Concepts for IMT-Advanced".

Keywords: WIMAX, amplifier, reconfigurable, power efficiency and linearity.

1 Introduction

Nowadays radio link design is targeting high peak data rates for high quality multimedia applications such as video, audio, animation, etc. In order to support these services, larger bandwidths and more complex modulations are required. Present wireless communications systems such as WIMAX, Wi-Fi and LTE employ orthogonal frequency division multiplexing (OFDM) as modulation technique to reach this aim.

OFDM has the ability to cope with severe channel conditions without complex equalization filters. However, an OFDM signal exhibits a high PAPR. In case of WIMAX signals, this value is around 8-10dB. Achieving simultaneously high efficiency and good linearity in power amplifiers design is the most challenging task.

Although typically energy efficiency has not stated as the main design criterion, it has been considered since the power consumption in mobile terminals is an actual bottleneck. The extension of the battery lifetime has been a design goal. One of the main factors involved in the success or failure of a radio technology is the performance of the high power amplifier. GSM uses low cost amplifiers due to the selected modulation, being this fact one of the reasons for its success. For example, LTE has adopted SC-FDMA in the uplink which reduces the PAPR requirement around 2-5dB compared with WIMAX, whilst maintaining OFDM advantages.

RF power amplifier designers are faced with this problem and different power efficiency enhancement techniques has been developed in [1], [2] and [3]. These techniques have been carried out to improve the efficiency of linear power amplifiers,

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 22–30, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

especially in the back-off region, where the power amplifier generally operates. Some examples are Envelope Elimination and Restoration (EER), Class F, Doherty and Envelope Tracking.

Most of these techniques involve complex architectures designs, and require the use of external control circuits and signal processing; except the Doherty topology which does not require any additional circuit. A Doherty power amplifier is a promising candidate having the advantage of high power added efficiency (PAE), low cost and simple implementation.

Under these statements, the design of a reconfigurable power amplifier for Mobile WIMAX applications based on the Doherty topology is considered as a demanding goal. The amplifier design is in 3.5GHz band, because it is the main frequency band for Mobile WIMAX applications in Europe. This frequency band covers from 3.4GHz to 3.6GHz. It is divided into uplink band (3400-3500MHz) and downlink band (3500-3600MHz) approximately. The present development has focused on the user terminal, so the design is set to cover the frequency band from 3400MHz to 3500MHz.

Apart from energy efficiency, reconfigurability is another important issue in power amplifiers. This is because potential adjustments in output power levels can lead to strategies using different cell sizes, network topologies, coordination between radio access technologies, etc. Therefore this feature was added to the power amplifier design requirements.

Along this paper, it is presented the design of a reconfigurable power amplifier for Mobile WIMAX, with some partial measured results. The final stage of the development phase will be addressed during the next year of the CELTIC project, MOBILIA.

2 WIMAX Reconfigurable Power Amplifier Design

Combining power efficiency enhancement techniques as the Doherty topology and power reconfigurability is a challenge to improve the battery lifetime in the user terminal. A design using both techniques was developed for Mobile WIMAX applications in 3.5GHz band.

In general, commercial WIMAX transceivers deliver around 0dBm output power, without a power amplifier. This paper has focused on the design of a power amplifier which can deliver up to 23dBm, typical value for mobile terminals, whilst maintaining a back-off not to distort the signal. The expected saturated output power is 30dBm, suitable to reach a trade-off between linearity and energy efficiency. Besides, power reconfigurability is added through an attenuator. The attenuator let the power amplifier be adjusted to different power scenarios and modulation levels. It is important to notice that the back-off will be different depending on the modulation level: QPSK, 16-QAM, or 64-QAM.

Following these requirements, the design presents in the following sections.

2.1 Doherty Amplifier Technique

Doherty technique was developed in 1936 for using in high-power broadcast transmitters [4]. Nowadays, it has found application in wireless communications due to its relative simplicity of implementation. It is an efficient method of using conventional linear amplifiers when operating with envelope-varying signals, such as WIMAX signals which exhibit high PAPR.

The basic concept behind the Doherty technique [5] is to allow one or more amplifiers to operate at their peak envelope power level and hence at maximum efficiency, whilst allowing a final linear amplifier to deal with the modulation peaks.

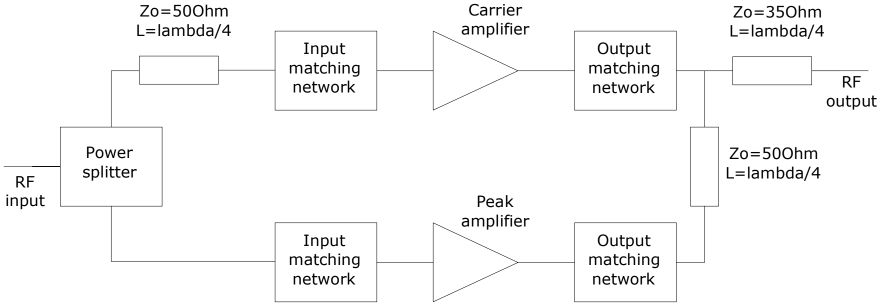


Fig. 1. Classical Doherty amplifier topology

Figure 1 presents a classical Doherty amplifier consisting of two amplifiers, namely the "carrier" and the "peak" amplifiers. These amplifiers are connected in parallel with their outputs joined by a quarter-wave transmission line, which performs impedance transformation. The "peak" amplifier delivers the current when the "carrier" amplifier saturates, thereby reducing the impedance seen at the output of the "carrier" amplifier. Thus, the "carrier" amplifier delivers more current to the load while it is saturated because of the load-pulling effect.

The performance of a two-stage Doherty amplifier can be defined in three ranges. The first one, it is the operation at low power levels, where the "peak" amplifier is shut down and the "carrier" amplifier is operating as a conventional linear amplifier. In the second range, it works at medium power levels and the "carrier" amplifier is saturated and acts as a voltage source; the "peak" amplifier takes over linear operation and acts as a controlled current source. And finally, as it operates at high power levels, both amplifiers are saturated, with the peak output voltage of the complete amplifier being the power supply voltage.

This configuration has a medium complexity, because of the relatively undemanding and low degree of required control. However, its main disadvantage is the narrow bandwidth performance because of the use of $\lambda/4$ transmission lines and the required phase accuracy between the two amplifiers.

As well as classical Doherty topology, some design methods have been studied to improve its performance and reduce its potential disadvantages [6], [7], [8] and [9]. One possibility is the use of individually optimized matching circuits in the "carrier" and the "peak" amplifier. Another method is the properly adjustment of the bias circuit to optimize the linearity and the efficiency. It is to be noted that an inverted Doherty topology can provide better efficiency. The theory indicates that the best efficiency at average envelop power is produced with a load impedance closer to 25Ohm than to 100Ohm. In this topology, the position of "carrier" and "peak" amplifiers are interchanged. Adding compensation lines and shunt capacitors to adjust phase in the circuit can improve linearity too.

Although some of the previously mentioned methods have been employed in this design, additional efforts will be made to improve the performance of the reconfigurable power amplifier.

2.2 Power Reconfigurability

Due to the limited power available in a user terminal, power reconfigurability is suitable to optimize energy resources for new multimedia applications. WIMAX Forum has published mobile radio specifications for WIMAX Release 1.0 [10]. According to these specifications, there are four power classes in WIMAX with different power level ranges from 18dBm to 30dBm approximately. Then adding power reconfigurability with an attenuation range lower than 12dB is an appropriate solution to save energy.

Furthermore, Mobile WIMAX standard incorporates mechanisms that enable subscriber terminals to be active only at certain times as negotiated with the base station. When there is no data to be transmitted or received, the subscriber terminal can move into sleep or idle modes to minimize power consumption. This characteristic will be proper to be implemented as well in the design in order to increase the battery lifetime.

Following these ideas, the power amplifier design incorporates an attenuator to be able to deliver the suitable power in each moment and to minimize power consumption and so extending battery lifetime. This option is adequate because the Doherty amplifier consumes according to its input power and this value can be adjusted through an attenuator combined with a driver amplifier.

Commercial WIMAX transceivers deliver around 0dBm, so about 30dB of gain for the reconfigurable power amplifier design would be enough. A Doherty amplifier using FPD1500SOT89 gets around 11dB of gain, so a driver amplifier in the order of 20dB of gain was selected, HMC326MS8G. This driver provides 22dB of gain and 26dBm of saturated power from a +5V supply voltage. It was optimized to provide greater than 40% PAE and has power down capability to reduce current consumption when the amplifier is not in use.

To adapt the power amplifier to different WIMAX power classes, an attenuator is introduced in the design, HMC540LP3. It is a 4-bit digital attenuator, with a total attenuation of 15dB (1dB LSS).

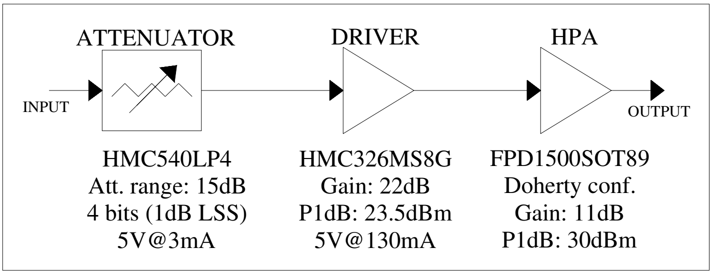


Fig. 2. RF block diagram of the reconfigurable power amplifier for Mobile WIMAX applications

As a result the reconfigurable power amplifier design is composed by a digital attenuator, a driver amplifier and a power amplifier based on the Doherty technique. Its main characteristics are 30dB of gain and 30dBm of output power with 12dB of attenuation range from 3.4GHz to 3.5GHz. Combining these components, the final amplifier is more efficient due to energy saving from Doherty technique and power reconfigurability. The block diagram of the proposed design including the selected components is shown in Figure 2.

Next sections present a detailed analysis of the reconfigurable power amplifier.

2.3 WIMAX Reconfigurable Power Amplifier Analysis

First of all, technical specifications for the amplifier design are stated. The frequency range will cover from 3400 to 3500MHz. Usually, it is the frequency band assigned in European Mobile WIMAX services to user terminals. Apart from that, WIMAX output power is between 18 and 30dBm to cover different power classes into the standard. Generic WIMAX transceivers deliver around 0dBm output power and WIMAX mobile stations typically transmit at 23dBm. Because of that a design with 30dB of gain and about 12dB in power adjustment is an appropriate goal.

In the first stage, a search for WIMAX commercial amplifiers in 3.5GHz band was carried out. In a Doherty amplifier, there are two amplifiers in parallel biased in class-AB and class-C, respectively. To model their performance, a non-linear model is required. Only RFMD, manufacturer of high-performance semiconductor components, provides a non-linear model that fits to the technical specifications, so the selected amplifier was FPD1500SOT89. The manufacturer provides a modeling report for FPD1500 TOM3 and TOM2 models. These models can be used in different microwave simulators and in this case the Advanced Design System (ADS) software was employed. Using these models, it is possible to simulate the full-scale device characteristics such as DC bias, gain, return losses, output power, efficiency (PAE), intermodulation, etc.

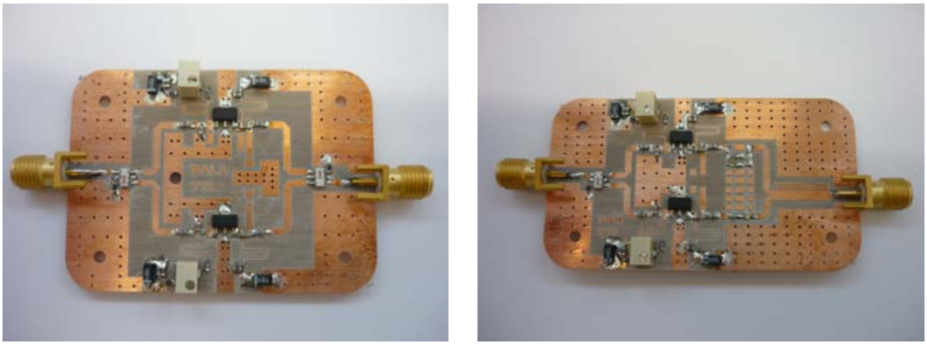
FPD1500SOT89 has 12dB of gain and 27.5dBm at 1dBcompression output power. It is biased by applying +5V and a negative voltage to get 200mA consumption in 3.5GHz band (class-AB).

A preliminary development of a Doherty amplifier using FPD1500SOT89 was carried out. A power splitter is required to separate the input signal into two ways with 90º phase shift. A 3dB 90º hybrid coupler can be used, QCN-45+ from Mini-Circuits. The rest of the circuit is designed using microstrip lines and passive components (capacitors, resistors and potentiometers). To compare Doherty amplifier results, a balanced amplifier was prepared in order to evaluate it in similar conditions.

The balanced amplifier has two amplifiers in parallel biased in class-AB. These amplifiers are combined using a 3dB 90º hybrid coupler at input and output ports.

The Doherty amplifier has two amplifiers in parallel biased in class-AB and class-C, respectively. The class-AB amplifier is biased as mentioned previously and the class-C amplifier is biased by applying +5V and a negative voltage to get 10mA consumption approximately. The main negative voltage in the circuit is -5V. The required negative voltage at the gate of the transistor is adjusted thanks to a potentiometer. In the case of 200mA, the negative voltage is around -0.5V, and it is -1V for 10mA.

In the following figures, photographs of these circuits are presented.



a) b)

Fig. 3. a) Balanced amplifier circuit using FPD1500SOT89 in 3.5 GHz band. b) Doherty amplifier circuit using FPD1500SOT89 in 3.5 GHz band.

The input structure in both circuits is the same, a 3dB 90º hybrid coupler. However, the output way presents some differences. In the balanced amplifier, a 3dB 90º hybrid coupler is employed again, while a λ/4 microstrip line with impedance transformation is used in the Doherty amplifier.

As it is presented in figure 3b), some compensation lines are used to fit phase in the Doherty amplifier in order to improve performance in the 3.5GHz band. This configuration presents a narrow bandwidth and it needs a specific adjustment. In the case of the balanced amplifier, the design has a large bandwidth, but it is not so energy efficient as the Doherty amplifier.

These circuits were measured in a radio frequency laboratory and the results are shown in the next section.

In a final design, the reconfigurable power amplifier will be integrated with a digital attenuator, a driver amplifier and a Doherty amplifier. In this document, only Doherty amplifier results are presented.

3 Performance Analysis

The design of the former amplifiers and the layout of their printed circuit boards were carried out thanks to linear and non-linear simulations realized in ADS. An S-parameters simulation was calculated to optimize the performance in frequency, and a Harmonic Balance simulation was done to improve the power performance. Figures 4 and 5 show the measured results of each amplifier. Both topologies have similar gain with good return losses. Something to be highlighted is that the balanced amplifier has return losses less than -20dB, while the Doherty amplifier has -10dB. The pseudomorphic high electron mobility transistor (pHEMT), FPD1500SOT89, is matched in each case through a shunt capacitor at input and a series capacitor at output to improve return losses.

ADS simulations had already presented return losses less than -20dB in the balanced amplifier from 3.4GHz to 3.5GHz and less than -10dB in the Doherty amplifier.

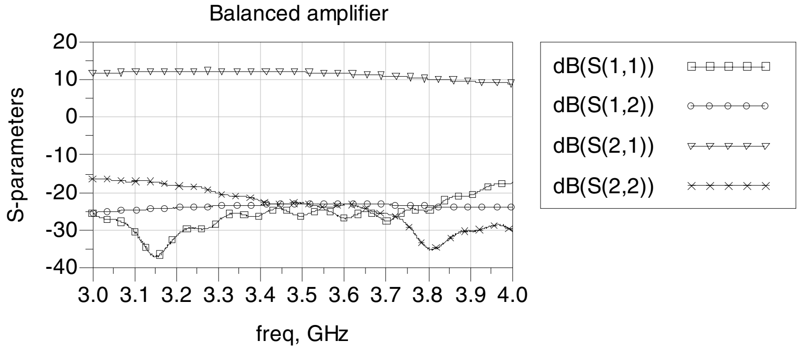


Fig. 4. Measured S-parameters results for the balanced amplifier using FPD1500SOT89

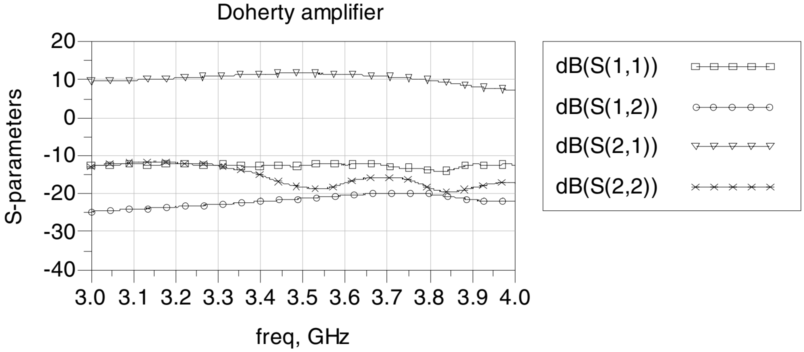


Fig. 5. Measured S-parameters results for the Doherty amplifier using FPD1500SOT89

Power measured results were obtained using an HMC326MS8G evaluation board from Hittite because of the available output power in typical RF generators is not enough to achieve the measurements properly. This driver amplifier, HMC326MS8G, has 22dB of gain and 23.5dBm of output power at 1dB compression. Using this amplifier combined with the balanced amplifier or the Doherty amplifier, it reaches more than 30dB of gain, enough for the reconfigurable power amplifier for Mobile WI-MAX applications.

In the next figures, gain and PAE are presented for the balanced amplifier and the Doherty amplifier. The balanced amplifier gives 29.6dBm of 1dB compression output power and 29.8dBm of saturated output power. Meanwhile, the Doherty amplifier provides a power output of 30dBm at 1dB compression output power and 30.2dBm of saturated output power. Maximum PAE in the Doherty topology is 40% as ADS simulations with TOM3 model presented and afterwards measurements have demonstrated. Both designs have similar gain. The Doherty design has around 0.5dB less gain than the balanced design. However PAE results are much better in the Doherty design compared with the balanced design. For example, for 23dBm output power, which is a typical value in mobile terminals, it is around 4% better. This power consumption improvement extend the battery lifetime which is a significant parameter for users. As size and complexity for both designs are quite similar, Doherty design becomes an interesting solution.

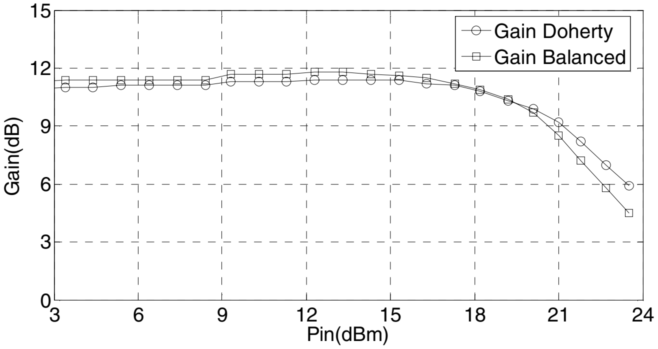


Fig. 6. Gain measurements versus input power for Doherty amplifier and balanced amplifier

Gain results are similar in both topologies and it can be observed than the Doherty amplifier provides higher output power. Besides, it is more efficient than the balanced amplifier as it is presented in Figure 7. Measurements are at 3.4GHz and results are similar from 3.4GHz to 3.5GHz.

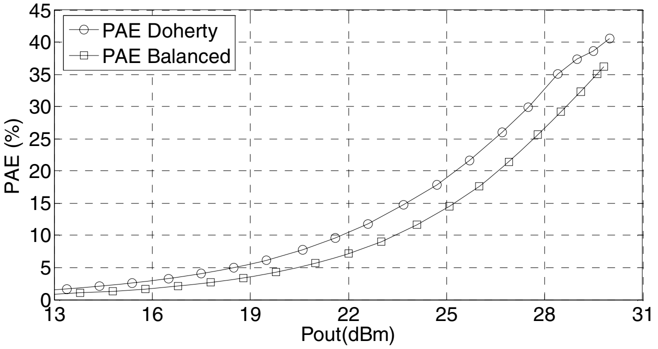


Fig. 7. PAE measurements versus output power for Doherty amplifier and balanced amplifier

In the Doherty design, offset lines were introduced to improve its performance adjusting phase shift between class-AB amplifier and class-C amplifier in 3.5GHz band. Furthermore, different polarization points for class-C amplifier were set to find the best results. Additional activities about this issue will be carried out during the project to find out the appropriate relation between efficiency and linearity.

4 Conclusions

A reconfigurable power amplifier for Mobile WIMAX applications has been designed based on a Doherty configuration. The Doherty amplifier technique can improve energy efficiency through an innovative topology of two parallel amplifiers biased in class-AB and class-C, respectively.

A balanced and a Doherty amplifier were fully developed and measured. Both designs use the same transistor, FPD1500SOT89, which is a high-linearity packaged pHEMT. Measurements show an improvement in PAE for the Doherty amplifier, implying an impact in battery lifetime, which is an important feature in user terminals. This improvement is around 4% of PAE for 23dBm output power, a typical output power in user terminals.

Apart from the Doherty amplifier, a driver amplifier and a digital attenuator is added to the system to integrate a reconfigurable power amplifier to be able to adjust the power to different scenarios. The same output power is not required all the time, it is better to fit the communication according to certain conditions as distance, number of users, quality of service, etc.

Final development and measurements will be carried out during next year of the project MOBILIA.

Acknowledgments. The research leading to these results has received funding from the Ministry of Industry, Tourism and Trade of Spain, subprogram AVANZA I+D nº TSI-020400-2008-52. MOBILIA project is in the framework of CELTIC program, whose proposal number is CP5-016.

References

1. Cripps, S.C.: Advanced Techniques in RF Power Amplifier Design. Artech House, Norwood (2002)
2. Raab, R.H., Sigmon, B.E., Myers, R.G., Jackson, R.M.: L-band Transmitter using Kahn EER Technique. IEEE Trans. Microwave Theory Tech. 46(12), 2220–2225 (1998)
3. Lepine, F., Adahl, A., Zirath, H.: A High Efficient LDMOS Power Amplifier Based on an Inverse Class F Architecture. In: 34th Eur. Microwave Conf. Amsterdam, the Netherlands, pp. 1181–1184 (2004)
4. Doherty, W.H.: A New High Efficiency Power Amplifier for Modulated Waves. Proc. of the Institute of Radio Engineers 24(9), 1163–1182 (1936)
5. Kenington, P.B.: High-linearity RF Amplifier Design. Artech House, Norwood (2000)
6. Kim, J., Cha, J., Kim, I., Noh, J., Park, C., Kim, B.: Advanced Design Methods of Doherty Amplifier for Wide Bandwidth, High Efficiency Base Station Power Amplifiers. In: 35th European Microwave Conference, Paris, vol. (2) (2005)
7. Chen, X., Guo, Y., Shi, X.: A High Linearity and Efficiency Doherty Power Amplifier for Retrodirective Communication. PIERS Online 4(2), 151–156 (2008)
8. Srirattana, N., Raghavan, A., Heo, D., Allen, P.E., Laskar, J.: Analysis and Design of a High-efficiency Multistage Doherty Power Amplifier for Wireless Communications. IEEE Transactions on Microwave Theory and Techniques 53(3), 852–860 (2005)
9. Cho, K.J., Kim, W.J., Stapleton, S.P., Kim, J.H., Lee, B., Choi, J.J., Kim, J.Y.: Gallium-nitride Microwave Doherty Power Amplifier with 40W PEP and 68% PAE. Electronics Letters 42, 704–705 (2006)
10. WIMAX Forum, `http://wimaxforum.org`

An Access Selection Prototype Based on IEEE 802.21

Bruno Cendón, Jesús Herrero, Ramón Agüero, Arancha Rodríguez, Santiago Albillos,
Javier Sainz, Aránzazu Sanz, and David Gómez

Avenida de los castros, s/n. CDTUC Fase B Módulo 5 39005 Santander (Cantabria) España
`ramon@tlmat.unican.es, sasaiz@creativit.com,`
`bcendon@tst-sistemas.es, jherrero@tst-sistemas.es,`
`arodriguez@tlmat.unican.es, jsg@creativit.com,`
`asanz@tst-sistemas.es, dgomez@tlmat.unican.es`

Abstract. The Mobilia project is facing the new challenges appearing in the forthcoming wireless communication scenarios in which one of the distinctive factors is their intrinsic and remarkable heterogeneity. The evolution of the technologies has brought about the possibility of having terminals equipped with different interfaces, and thus the end-user device should be able to select the most suitable from a broad range of access alternatives. This paper presents an illustrative use case, based on a businessperson who presents different communication needs while traveling through heterogeneous networking scenarios. Starting from this point, we derive a set of requirements which should be addressed by Mobilia, following the concept of always best connected. Finally, the paper presents a platform developed so as to evaluate the entities performing the mobility management, handover decision algorithms and architectural protocol extensions, as proposed in the project.

Keywords: Service platforms, Validation, Demonstration, Heterogeneous accesses, Media Independent Handover, Mobility.

1 Introduction

One distinctive characteristic of future network deployments in wireless communications is their intrinsic heterogeneity. This does not only affect the involved technologies, but it also spans to the operators behind the different networks. It is envisaged that current performance figures would not be enough to fulfill with the new expectations so it is required to study advanced techniques and new algorithms in order to improve the mechanisms which are employed to select the most appropriate access. Hence, it is quite sensible to assume that, in order to offer end-users a good service, different actors might need to cooperate between them.

After analyzing the requirements obtained from the proposed scenarios, Mobilia suggests a new architecture able to handle the identified challenges. Due to its growing relevance, it uses the framework provided by the IEEE 802.21 group, the Media Independent Handover as the transport mechanism for the signaling which will be required between the involved entities. The information carried over such messages will be used to foster an optimum access selection.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 31–42, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

Another key element to be studied and evaluated in this work is the service platform. In order to offer the users the best Quality of Service (QoS), it is mandatory to adapt their performance to the characteristics of the subjacent wireless technologies, in terms of load, quality, etc. This implies that there must be some sort of interaction between the service platform and the access selection architecture.

The paper is structured as follows: Section II presents an illustrative use case where a businessperson presents different communication needs while traveling through heterogeneous networking scenarios. Based on these scenarios, section III introduces the requirements and concepts to be evaluated. Section IV describes the demonstrator process, based on a concrete use case derived from the first scenario. Finally, section V summarizes the main conclusions of this work.

2 Scenarios

This section describes a day-in-the-life of a business person. By looking at her necessities, we will be able to identify the communication requirements that Mobilia project needs to deal with. Before, we present the technical assumptions which must be taken into account.

2.1 Assumptions

The most important part of the scenario is the mobile terminal, since it is assumed to have the capacity to seamlessly interact with a number of new and legacy wireless technologies, including UMTS, HxSPA, LTE, WiMax and 802.11. As will be detailed later, this relevant heterogeneity needs to be emulated on a real platform, due to the limited availability of these technologies (especially if we are willing to integrate them with proprietary developments and procedures).

Regarding the services which will be involved, it is worth highlighting their broad set of different requirements, such as high speed, low delay, etc, (imagine e.g. video conference and high quality video streaming). We could even envisage some sort of business cases, considering several subscribers; whose are able to obtain a premium service by the reservation of the appropriate bandwidth required for their specific services/applications needs.

The scenario describes how these Premium services are launched. In the meantime, we would assume that the terminal is able to operate in a power saving mode, while being aware of new video calls or other services.

2.2 Story Line

The use case presented in Mobilia follows the story line of a businessman, John, travelling from Madrid to Bilbao for a meeting. The user owns a Personal Area Network (PAN) which consists of a laptop (WLAN, Bluetooth) and a Smartphone (that could be a; WLAN, UMTS, Bluetooth and WiMax).

John starts the journey connected to the Internet via the WiFi home network, so he establishes a conference with his colleagues in Bilbao and closes the agenda for the meeting in the afternoon. One hour later, just before leaving the house John shuts down the laptop, the PAN recognizes the action and transfers the conference to his

Smartphone. Until this moment the PAN is connected via the WiFi network and just before leaving the coverage area, the Smartphone starts to search new available networks (UMTS, WiMax) in order to continue the conference started earlier.

Once in the car, all the Smartphone functionalities are transferred over Bluetooth to the small remote control located on the steering wheel. John is able to continue with the conference using the hands-free mobile kit while the Smartphone connects to the company network, and starts to synchronize his corporate mailbox in the background.

The next step in the journey is a shopping centre. While John is having the breakfast in a coffee shop, the Smartphone detects a local Hot-Spot network which allows internet access with lower costs than UMTS technology and with a higher Quality of Service, so John finishes the conference using this access. During all this time he has been receiving offers to download multimedia contents over a podcasting service. On the other hand, the "hot-spot" detects John´s laptop relaying capabilities so he is offered a discount on his connection if he makes the laptop work as a relay node extending the coverage of the station hot-spot to other end-users.

Finally, he arrives at the airport and starts a new connection to the internet using a WiFi hotspot. Since the WiFi hotspot is heavily loaded, and provided that Madrid airport offers a WiMax access network, John is able to access the news, update the Smartphone, and use all the Internet services he needs until boarding time using this alternative access.

3 Requirements and Concepts to Be Evaluated

The Mobilia Project, based, among others, on the previously identified challenges, is focusing on some of the technologies and general system requirements and features from what we refer to as IMT-Advanced [1]: below we enumerate some of the most relevant ones.

- Access and Handover Latencies to enable delay-sensitive applications.
- Support of Traffic classes with different latency and packet error rates performance, in order to meet the end-user QoS requirements for the various applications.
- Mobility environments (pedestrian, vehicular and high speed) Optimization for specific low speed scenarios.
- Global roaming capabilities.
- Mobile user interface. Ubiquitous access, support for unicast and multicast broadcast services.
- Peak and sustained data rates, capacity, latency, overall network complexity and QoS management.
- Based on open standards and protocols.
- Supporting state of the art and legacy applications as video, web browsing, e-mail, file uploading and downloading, streaming video and audio, Location based services, Voice Over IP (VoIP), instant messaging and on-line multiplayer gaming.

The Mobilia solution supports the "always-on" paradigm based on two distinctive factors: the smart administration of the mobile energy and the support to a user experience of moving seamlessly between heterogeneous mobile access technologies. In particular, Mobilia is focusing on the following technical goals.

- To achieve the capacity to seamlessly interact with a number of new and legacy heterogeneous wireless technologies.
- To avoid interferences and collisions at the physical layer (technologies with different frequency bands and power transmission).
- Lower delay, higher QoS, power saving strategies and improve energy efficiency.
- Use the standard IEEE 802.21 in order to facilitate the exchange of information process and help to improve it.

4 Demonstrator: Service Networking Components for Heterogeneous Accesses

Derived from the scenario which has been depicted above, this Section presents the architecture that has been designed in order to assess the feasibility of the previously identified concepts. It is important to remark that its main goal is to assess their feasibility over real platforms. Hence, the existing clear limitations regarding the technologies to be used need to be taken into consideration. We have to recall that, at the time of writing, the availability of cellular (and WiMax) communication infrastructures is difficult to be ensured, especially if we think about the possibility of modifying their legacy operation during the access selection (resource management) procedures, as will be further explained later.

We understand that a clear added value of this proof-of-concept platform is the role that the Media Independent Handover Function (MIHF) plays [2]; we have already seen that IEEE 802.21 will be of outer relevance in handling heterogeneity in forthcoming wireless communication scenarios. Although there are some recent works which have already provided some details about IEEE 802.21 implementation, we go beyond them, since we analyze its role on a particular use case and, furthermore, we extend its original purpose, by using it so as to handle message interchange between the entities which are within the same node.

4.1 Platform Implementation

The Mobilia Demonstrator comprises a number of off-the-shelf components, over which some of the concepts developed within the Mobilia Project, and which have been previously detailed, can be assessed and evaluated. As we have introduced before, this platform must take into account the limitations of the available technology, in order to establish some bounds on the degree of detail which is sensible approaching for the different aspects to be challenged.

The idea of using "real" heterogeneous networks (meaning completely different technologies) needs to be discarded, due to its inherent complexity and extremely high cost (UMTS licenses, etc). Moreover, the necessity of incorporating our own developments within the Access Points prevents the use of commercial products. For instance, currently available WiMAX equipments and their corresponding software are not open enough to allow modifying their legacy operation. On the other hand, the architecture, both at a conceptual and at an implementation level, is flexible enough so as to enable the integration of additional technologies, if it was deemed necessary. The use of 802.21 ensures this degree of flexibility, although the limitation is more on the availability of the required products, Operating System support and possibility to tailor the legacy behavior of the network-side elements.

As a consequence, heterogeneous networks are emulated within the platform. We will use two different WiFi Networks (IEEE 802.11b and IEEE 802.11g) so as to guarantee a certain heterogeneity level (the two corresponding WLAN cells are configured in different and non-overlapping channels).

Traditional laptops are used for all the nodes which are part of the platform. All of them are running the Linux Operating System [3] (Ubuntu distribution) and use both their internal WiFi chipsets (Intel) as well as an external PCMCIA cards, based on the Atheros chipset. These wireless cards are essential, since they allow us the use of the *MadWiFi [4]* drivers and emulate the role of Action Point (AP) within traditional laptops.

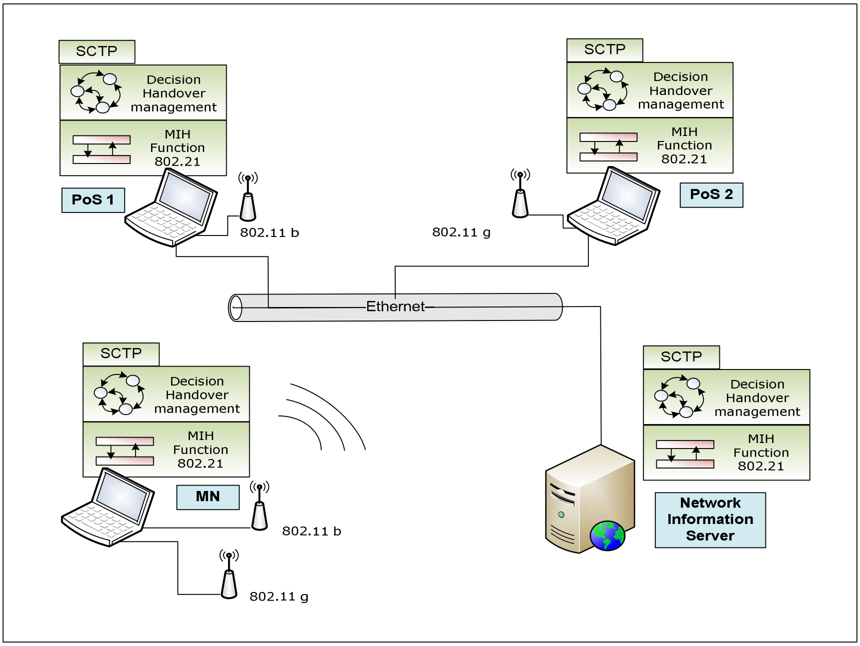


Fig. 1. This Figure depicts the demonstrator architecture used in Mobilia project

The figure 1 shows the architecture and equipment involved in the development of Mobilia demonstrator [5]. First, on the end-user side, we have the *Mobile Node* (MN). It is represented by a laptop which incorporates two WiFi cards. On the network side, there are two laptops working as the two different *Points of Services* (PoS) and a *Network Information Server*, which exchanges information with the other entities. The two access elements are configured to emulate heterogeneous technologies, and thus they use non-overlapping channels, while the *Network Information Server* resembles the role of an Access Broker, able to assign resources based on the information it is aware of as well as its own rules and policies.

From a software perspective all the different nodes, incorporate a number of independent processes which interchange information between them. In particular, the following components, which emulate the Mobilia architecture to deal with heterogeneous accesses.

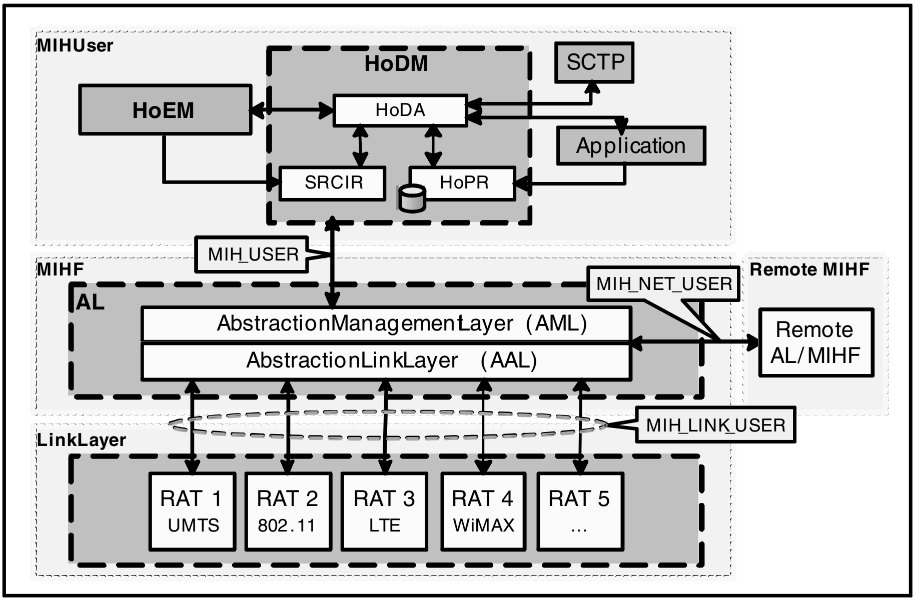


Fig. 2. The architecture proposed for Mobilia will inherit the framework defined by 802.21, creating on top of it a dedicated system to manage the information collection and management, the handover decision and its proper execution

We briefly describe the role of each element represented in figure 2, and afterwards, we provide some additional insights about them,

- Link Layer: Based on the MIH_LINK_USER SAP defined on the IEEE 802.21 specification, it facilitates to the different Radio Access Technologies (RATs) the data exchange with the Abstraction Layer.
- Abstraction Layer (AL): Its main function is to enable, either locally or remotely, the exchange of information and commands between the different devices involved in making handover decisions and executing handovers. It enables a fair and technology-agnostic comparison of the characteristics of the subjacent radio technologies.
- Remote MIHF: Provides to the framework the capabilities to share relevant information with remote elements through the MIH_NET_USER SAP.
- Decision Handover Management (HoDM): Based on the information provided by the Abstraction Layer through the MIH_USER SAP and a number of rules and policies, it takes a decision on which is the most appropriate access alternative.

- Stream Control Transmission Protocol (SCTP): It is a reliable, general-purpose transport layer protocol for use on IP networks that addresses mobility needs

IEEE 802.21 Signalling. One of the most important aspects of the demonstrator is the use of IEEE 802.21 as a transport medium for the exchange of information between different entities in the network [6]. The use of this standard will help to provide as much information as possible to the *Handover Decision Manager*, optimizing the decisions regarding the access point to be connected each time. The IEEE 802.21 signaling is based on a Type-Length-Value (TLV) codification, which offers different advantages from the point of view of implementation.

Abstraction Layer. The Abstraction Layer implements the 802.21 Media Independent Function, allowing the Handover Decision Manager to retrieve relevant information (and to instruct actions related to the handover process) from the different technologies its own device is equipped with, as well as with other network elements if needed.

More specifically, the Abstraction Layer (AL) designed within the Mobilia framework will be a custom implementation of the MIHF layer defined in IEEE 802.21 standard. It is structured into two different components, the Abstraction Management Layer (AML) and the Abstraction Link Layer (ALL)

The *Abstraction Management Layer* is in charge of managing the User MIH interface (MIH_SAP) and the remote interface (MIH_NET_SAP).

The *Abstraction Link Layer* manages the interfaces with the Link Layer (MIH_LINK_SAP).

For each Service Access Point (SAP) there are a group of primitives defined that are described in [6].

Handover Decision Management. The Handover decision management is performed by two elements: The *Handover Decision Manager (HoDM)* and the *Handover Execution Manager (HoEM).*

Handover Decision Manager:

The HoDM is the core part of this entity, being the element with the final responsibility during the execution of the handover. All the data meaning and decision criteria are located at this level of the architecture. It is composed by the following elements:

- *Handover Decision Algorithm Module.* This HoDA element includes the necessary intelligence to decide when a handover shall be done.
- *Handover Policies Repository.* This HoPR repository is used by the HoDA to set the basis of the conditions to order a handover. This information is combined with the one provided dynamically by the Service Requirements Collector Information Repository (SRCIR).
- *Service Requirements Collector Information Repository.* The SRCIR implements the MIH_USER interface to the AL/MIHF and act as a dynamic repository for the information collected from the MN and the Network. This information is used by the HoDA.

Handover Execution Manager:
The HoEM interfaces directly with the MIHF through the SRCIR to manage the primitive exchange in order to execute the handover. This element owns the necessary intelligence to manage the event reporting and error handling that the handover procedure might create.

SCTP Protocol. As previously mentioned, SCTP is a transport layer protocol for IP networks. While the protocol was originally designed for telephony signaling (under the RFC 2960 [7]), SCTP provided some interesting additional functionalities. It solved some of the limitations of Transmission Control protocol (TCP) while borrowing beneficial features of User Datagram Protocol (UDP). SCTP [8] allows high availability, increased reliability, and improved security for socket initiation.

Mobilia will use SCTP as an alternative mobility mechanism to Mobile IP. The utilization of SCTP tries to explore alternative solutions to the wasteful use of bandwidth and the IP tunneling by Mobile IP that is forcing a lot of communications to go back and forth to the Home Agent location. In the case of high throughput communications like those proposed by IMT-Advanced this should be avoided if possible. The solution proposed should provide as well faster handover speeds as the ones provided by Mobile IP due to the intrinsically lower layer mechanisms involved.

Mobilia A SCTP proxy will be used at both sides of the channel. In the server side it takes an incoming UDP connection, establishing an outgoing SCTP connection. In the client side the process operates reciprocally; it takes an incoming SCTP connection and sends the data flow through an outgoing UDP connection .This solution has been selected in order to be able to use a standard video server and client such as the VideoLAN Client (VLC) media player. The SCTP proxy in the client has also a thread to test if one of its interfaces must be in the SCTP association and change it.

The distinctive capability of SCTP entailing it as a mobility solution is its multihoming capacity. Multi-homing provides applications with higher availability than those that use TCP. A multi-homed host is one that has more than one network interface and therefore more than one IP address to which it can be addressed.

SCTP supports mobility because it does not require additional equipment such as the Home Agent of Mobile IP.

The last version of SCTP protocol is defined by RFC 4960 [9], and the optional extension for Dynamic Address Reconfiguration is defined by RFC 5061 [10]. This extension will allow an SCTP stack to:

- Dynamically add an IP address to an association.
- Dynamically delete an IP address from an association.
- Establishing the primary address the peer will use when sending to an endpoint.

These characteristics are also especially useful in handover scenarios, since they allow dynamic changes in the connection even if the terminal has only one interface. As a conclusion STCP provides features demanded by IMT-Advanced like lower latencies and seamless connectivity [1].

4.2 Use Cases

Looking back to the story line, we can extract three different use cases [11]:

- *Use case A* corresponds to the moment when the businessman in the middle of a conference shuts down the laptop and the conference is automatically transferred to the Smartphone. This time, the decision of execution of the handover comes from the user side.
  This use case will be represented in the proof of concepts through a handover process from IEEE 802.11g to IEEE 802.11b (in place of UMTS) which will be initiated by a "Link going down" primitive.
- *Use case B* corresponds to the moment when the businessman arrives to the shopping centre and the Smartphone (connected by UMTS) detects a local Hot-Spot network which allows Internet access with lower costs than UMTS technology and without downgrading the current Quality of Service. As a consequence, the Smartphone will change to the Hot-spot network.
  This use case will be represented in the proof of concepts through a handover process from IEEE 802.11b (in place of UMTS) to IEEE 802.11g which will be initiated by an application which requires more bandwidth and "prefers" lower costs.
- *Use Case C* matches the last handover process detailed in the scenario, when the businessman is in the airport using a WiFi connection which is suffering from a high load situation; in this case the handover process is initiated by the Serving Network. This time the handover is from WiFi to the WiMAX access network provided by the airport [12].
  This use case will be represented in the proof of concept by means of a handover process from IEEE 802.11b to IEEE 802.11g (instead of WiMax) which will be initiated by the Network Information Server.

In the following, we provide a detailed description of the first use case, in which we depict all the primitives and components which take part on the whole process.

Use Case A: Flow Chart. The next figure shows a Handover process from IEEE 802.11g to IEEE 802.11b motivated by a *Link going down* event. This flow chart is emulating the handover process in the use case when John leaves his home and there is a handover process between WLAN and UMTS. The first step in the process is making a subscription to the events that the MN wants to receive in the future. A *MIH_Link_Parameters_Report* is generated when one of link parameters (e.g., the speed of link, QoS, and bit error rate) equals to a given threshold value set by *MIH_Link_Configure_Thresholds* command. This information goes up to the HoDM that will decide to have a handover. Right after that, the Mobile Node sends a *MIH_Get_Information* request frame to the Network Information Server. Then, it sends back a MIH_Get_Information.response frame which contains the available neighboring networks information [6].

This information is also forwarded to the HoDM, which decides to go on with a given list of potential candidate networks. To do so it sends a request to its serving PoS (located on 802.11 g Point of Service). This information is sent using the primitive *MIH_MN_HO_Candidate_Query.request*. Then, the serving PoS starts querying the available candidate networks (taking into account the information provided by the MN) asking for the list of resources available and including the QoS requirements of the user, this is performed by a successive exchange of *Query Resources* messages with one or several candidate PoSs (only with another PoS in our case). The result of

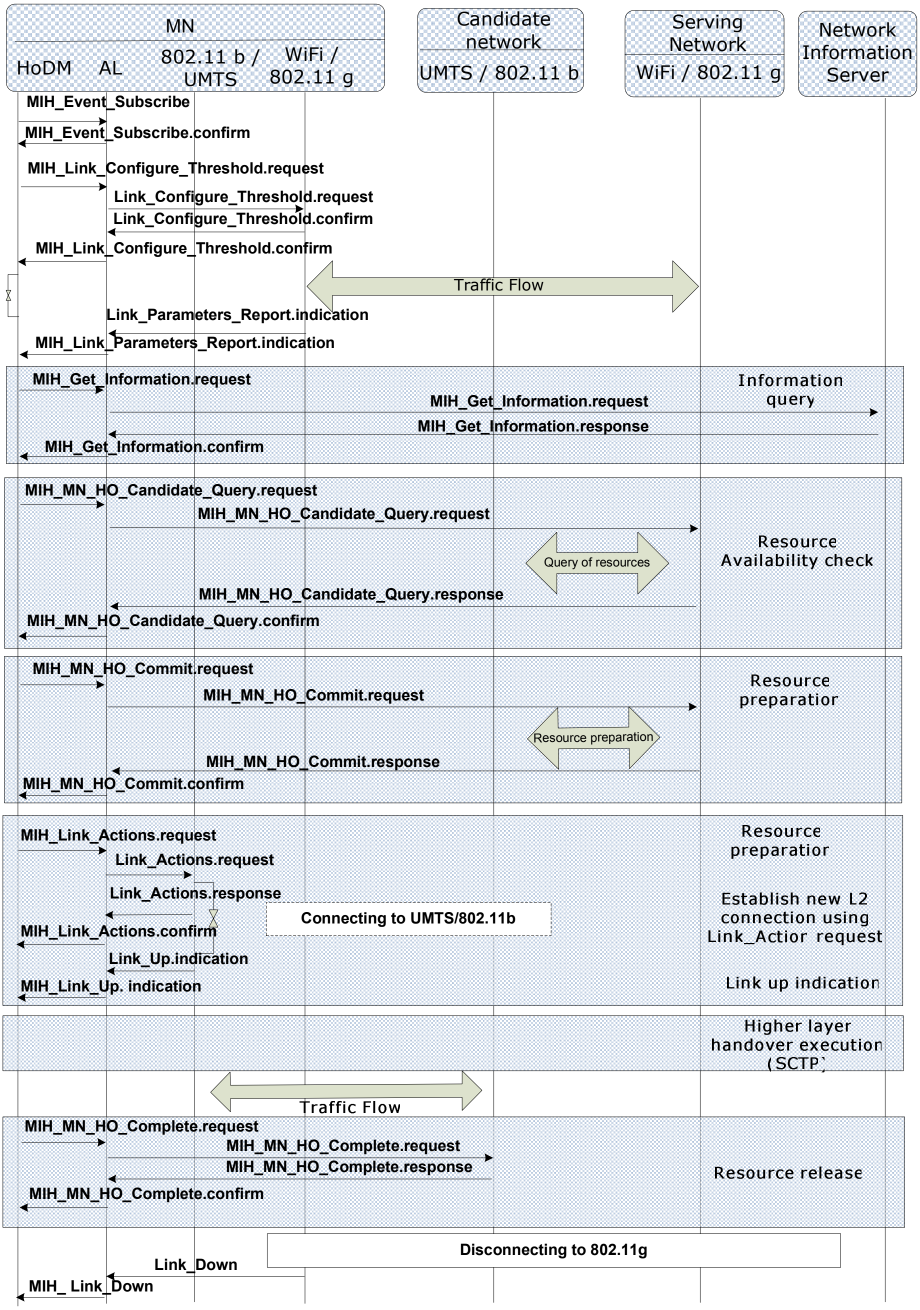

MN
HoDM
AL
802.11 b / UMTS
WiFi / 802.11 g
Candidate network
UMTS / 802.11 b
Serving Network
WiFi / 802.11 g
Network Information Server
MIH_Event_Subscribe
MIH_Event_Subscribe.confirm
MIH_Link_Configure_Threshold.request
Link_Configure_Threshold.request
Link_Configure_Threshold.confirm
MIH_Link_Configure_Threshold.confirm
Traffic Flow
Link_Parameters_Report.indication
MIH_Link_Parameters_Report.indication
MIH_Get_Information.request
Information query
MIH_Get_Information.request
MIH_Get_Information.response
MIH_Get_Information.confirm
MIH_MN_HO_Candidate_Query.request
MIH_MN_HO_Candidate_Query.request
Query of resources
Resource Availability check
MIH_MN_HO_Candidate_Query.response
MIH_MN_HO_Candidate_Query.confirm
MIH_MN_HO_Commit.request
MIH_MN_HO_Commit.request
Resource preparation
Resource preparation
MIH_MN_HO_Commit.response
MIH_MN_HO_Commit.confirm
MIH_Link_Actions.request
Resource preparation
Link_Actions.request
Link_Actions.response
Connecting to UMTS/802.11b
Establish new L2 connection using Link_Action request
MIH_Link_Actions.confirm
Link_Up.indication
MIH_Link_Up. indication
Link up indication
Higher layer handover execution (SCTP)
Traffic Flow
MIH_MN_HO_Complete.request
MIH_MN_HO_Complete.request
MIH_MN_HO_Complete.response
Resource release
MIH_MN_HO_Complete.confirm
Disconnecting to 802.11g
Link_Down
MIH_ Link_Down

Fig. 3. This shows the flow chart concerning the Handover process from 802.11g to 802.11b motivated by a *Link going down* event [6]

the queries is sent to the MN through *MIH_MN_HO_Candidate_Query.response*. At this point, the MN owns enough information about the surrounding networks to take a handover decision.

Once the HoDM, Handover Decision Manager, has decided the target network to handover, the HoEM takes command of the situation and delivers this information to the Serving network using *MIH_MN_HO_Commit.request* which will exchange some information with the candidate network and will send a confirmation to the Mobile Node through *MIH_MN_HO_Commit.response*. The next step is establish new L2 connection using *Link_Action.request* and after issuing the commands to start UMTS/802.11 b connection establishment, the AL sends a message to the HoDM indicating the start of the connection. Then, there is a *Higher Layer Handover Execution (SCTP)* and the HoDM sends an MIH_HO_Complete message to the AL, which will inform the target PoS, which becomes the new serving PoS. Finally, there is a disconnecting process in the old serving network which finishes with a *Link_down* message.

5 Conclusion

The advent of heterogeneous wireless networks is already a reality. This has brought about the need for architectures able to deal with the upcoming challenges and requirements which will appear. Although there has been already some works proposing solutions towards this direction, most of them have not studied their feasibility over real platforms. We understand that this is a mandatory step, since we might obtain information elements so as to refine and fine-tune such architectures. In the Mobilia project we have faced this challenge and we have designed and implemented a demonstrator, using off-the-shelf technologies and components to assess the feasibility of the proposed architecture.

A number of use cases were established over a typical scenario (a day in the life of a business man), so as to identify the necessities and requirements which should be tackled by the Mobilia architecture. This scenario has been mapped onto a real platform, taking into consideration the limitations of existing technologies, and over such platform, different entities have been tested.

The demonstration encompasses various entities, both at the end-user and network side, and handles access selection based on different parameters, such as link quality and network load. In addition, different rules and policies can be established, based e.g. on the operator agreements and end user preferences.

One of the main contributions of the Mobilia architecture, in general, and in the demonstration, in particular is the role that it has been given to the Media Independent Handover Framework. It goes without saying that the work carried out by the IEEE 802.21 working group will play a key role in heterogeneous networking scenarios, and thus it is interesting assessing its feasibility over real platforms. In the presented demonstrator, the IEEE 802.21 specification has been used so as to handle the signaling interchange between the different Mobilia components.

Mobility is another feature which cannot be avoided in the considered scenarios; in order to handle IP addresses while shifting from one access to another, we have employed SCTP, although the architecture is flexible enough to use other solutions. The most remarkable aspect is that the mobility solution has been integrated the access selection engine, and reacts to its requests.

This platform will be extended, so as to be able to analyze different situations and algorithms. In addition, the conclusions which can be extracted from it will allow us to refine and fine-tune the proposed architecture, together with the simulation-based analysis which is being carried out in parallel.

Acknowledgements

All authors would like to express their gratitude to the Spanish government for its funding in the Mobilia (CELTIC Program) project, (Avanza I+D TSI-020400-2008-82). Ramón Agüero would also like to thank the Spanish Government (Ministerio de Ciencia e Innovación) for its funding in the project "Cognitive, Cooperative Communications and autonomous SErvice Management", C3SEM (TEC2009-14598-C02-01)

References

1. IMT –ADVANCED 8F/IEEE-3-E 15 ITU (2007)
2. Purkayastha, D., Carlton, A.G.: A Tutorial on IEEE 802.21, Media Independent Handover Services (2006)
3. Piri, E., Pentikousis, K.: Towards a GNU/Linux IEEE 802.21 implementation. In: Proc. IEEE International Conference on Communication (ICC), Dresden, Germany (2009)
4. The madwifi project (2010), `http://madwifi-project.org`
5. Mobility Concepts for IMT-Advanced (Mobilia) Project "Platform description", D5.1 (2009)
6. IEEE P802.21: Standard for Local and Metropolitan Area Networks: Media Independent Handover Services. LAN MAN Standards Committee. IEEE Computer Society (2009)
7. RFC 2960: Stream Control Transmission Protocol, IETF Network Working Group (2000)
8. Jones, T., Emulex, M.: Better networking with SCTP The Stream Control Transmission Protocol combines advantages from both TCP and UDP IBM Solutions (2006)
9. RFC 4960: Stream Control Transmission Protocol, IETF Network Working Group (2007)
10. RFC 5061: Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration (2007)
11. Buburuzan, T., May, G., Melia, T., Mödeker, J., Wetterwald, M.: Integration of Broadcast Technologies with Heterogeneous Networks – An IEEE 802.21 Centric Approach (2008)
12. Lopez, Y., Robert, E.: Open MIH, an Open-Source Media-Independent Handover Implementation and its Application to Proactive pre-Authentication. In: Proc. of the First International ICST Conference on Mobile Networks and Management, MONAMI 2009, Athens, Greece (2009)

Multi-hop Extensions to Heterogeneous Access Network Selection

Ramón Agüero, Johnny Choque, and Luis Muñoz

University of Cantabria, Santander, Spain
`ramon@tlmat.unican.es`

Abstract. This paper evaluates an access selection architecture able to handle heterogeneous technologies. We establish a generic access selection algorithm, which assigns different weights to the constraints established by both the network and the terminal. In addition, we improve the traditional operation by allowing multi-hop extensions, by means of which an end-user may reach an Access Element (i.e. base station) through other nodes willing to relay traffic. The results show that the multi-hop extensions are beneficial, not only from the point of view of the end-user, but also from the perspective of the network operator, since they allow an increase on the overall network throughput.

Keywords: Heterogeneous Access Networks, Multi-hop extensions.

1 Introduction and Related Work

Near future wireless communications will be characterized by being highly heterogeneous, not only regarding the involved technologies, but also considering the number of operators which will manage the different networks. In such scenarios, the end-user would have a much wider choice than today. This has gathered the interest from both the scientific community and the relevant standardization bodies. In fact, this has brought about several research challenges which have been covered just partially, and thus it is worth considering them.

Thanks to the recent proliferation of different radio access technologies, together with the advances on electronic miniaturization, it is nowadays becoming more common to have devices able to communicate over different technologies. In parallel, due to the rise of the number of network operators, as well as the increasing requirements from the end-user services, it is clear that some sort of cooperation between networks might be required.

Although this line of research has attracted much interest, most of the existing works are focused on a subset of the whole problematic, without looking at it with a holistic view. A first point which becomes fundamental is the abstraction of the subjacent resources, so that they could be managed on a homogenous and uniform way (see, e.g. [1], [2], [3], [4]). In this aspect, it is also worth highlighting the effort being made by the IEEE 802.21 group, which is currently defining a framework to ease the handover processes between networks, on an independent way from the subjacent technology (Media Independent Handover Services).

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 43–56, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

The current "almost-static" access selection which is used by most of the current technologies and networks would most likely become insufficient in the future; in fact, it will be required to change the current access, based on various parameters, such as the end-user preferences (policies) or the current situation of the network (in terms of e.g. load). Due to this new challenge, an entity able to collect, classify and deliver those events, which might eventually evolve into an access change (see [5]), is needed.

Another aspect which is common to all the different proposals which have been done within this line of research is a smart entity, able to process all the available information, providing the user with the best possible access any time. This component has received different names, such as MRRM [6], [7], CRRM [8], JRRM or CARM [9], although all of them share the same basic characteristics and functionalities.

There exist a number of works which can be embraced within this framework. In [10], the authors present an architecture to perform access selection within heterogeneous network environments. Other focus on particular technologies, like [11], [12], [13], which mostly analyse the integration between WLAN and 3G, studying different mobility schemes; furthermore, [14] discusses the benefits of employing different metrics to determine the optimum access, although they do not consider the possibility of changing one access once it has been selected. The approach followed by the AROMA project should be also highlighted [15], since it follows the guidelines proposed by the 3GPP [17] group and it focuses on the integration of UMTS and WLAN technologies. We must say that this paper does not aim at proposing a novel architecture, but it extends previous works since it carries out a thorough analysis of access selection algorithms which could be brought about by such frameworks.

Hence, we will use a simulation-based approach to evaluate the access selection architecture developed within the Mobilia collaborative project [16]. A generic algorithm has been designed, able to assign different weights to the constraints established by either the network or the end-user terminal. Furthermore, one of the distinctive features of the analysis is that we extend the more traditional approach, by means of multi-hop extensions, as long as the end-users have the opportunity to reach a base station by means of other entities willing to relay traffic.

The paper is structured as follows: Section 2 presents the algorithm which will be evaluated. Section 3 introduces the configuration and parameters of the proprietary simulator which has been developed to carry out this analysis, whose results are reported in Section 4. Finally, Section 5 concludes the paper, advocating some items for future work.

2 Access Selection Algorithm

This section presents the access selection algorithm which will be evaluated, taking into consideration the constraints of both the network and the end-users, *Network Constraints (nc)* and *Terminal Constraints (tc)*, respectively. A different weighting factor will be applied to each of these parameters and, finally, the

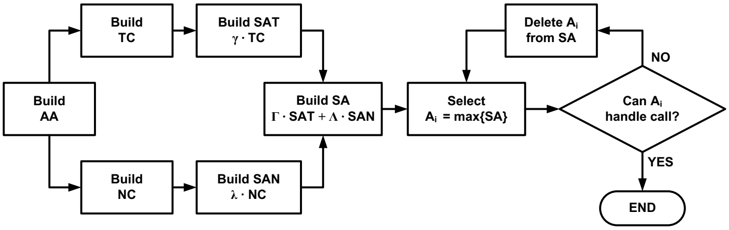


Fig. 1. Access Selection Algorithm

preferences of both entities will be combined, selecting the access alternative which maximizes the resulting cost function. Particularly, a linear combination of the constraints will be used so as to evaluate each of the elements detected by the terminal, as it is shown in (1), where A_j refers to the suitability of access j to the user.

$$A_j = \Gamma \sum_{i=0}^{N} \gamma_i tc_i^{(j)} + \Lambda \sum_{i=0}^{M} \lambda_i nc_i^{(j)} \tag{1}$$

In the previous expression, Γ refers to the overall weight which is given to the terminal (end-user) preferences, while Λ modulates those aspects which affect the network. Furthermore, a different weight is applied to each of the parameters (γ_i for the different terminal constraints and λ_i for the network ones), which will be used so as to adjust each of the j^{th} access constraints, ($tc_i^{(j)}$ and $nc_i^{(j)}$, respectively). Thus, N is the overall number of constraints handled by the terminal, while M refers to the constraints handled by the network. The value of A_j lies between 0 and 1, provided that the values of all the different weights are properly selected.

In this sense, Figure 1 depicts the access selection algorithm. As can be seen, it starts with the establishment of the Available Accesses (AA) set. It embraces all the Access Elements to which the end-user has a possibility to connect. On a traditional system, this set will contain those base stations covering the position of the end-user; however, we also account for the possibility of connecting with an Access Element by means of a multi-hop path, if there are some nodes willing to relay traffic. Starting from this set, both the network and the terminal build their corresponding constraint matrixes (**NC** and **TC**, respectively), where each of the columns comprises the constraints which are being applied to each of the T elements of the AA; they apply those matrixes to build their corresponding Selected Accesses (SAN and SAT).

$$\mathbf{TC} = \begin{bmatrix} tc_1^{(1)} & tc_1^{(2)} & \cdots & tc_1^{(T)} \\ tc_2^{(1)} & tc_2^{(2)} & \cdots & tc_2^{(T)} \\ \vdots & \vdots & \ddots & \vdots \\ tc_N^{(1)} & tc_N^{(2)} & \cdots & tc_N^{(T)} \end{bmatrix} \qquad \mathbf{NC} = \begin{bmatrix} nc_1^{(1)} & nc_1^{(2)} & \cdots & nc_1^{(T)} \\ nc_2^{(1)} & nc_2^{(2)} & \cdots & nc_2^{(T)} \\ \vdots & \vdots & \ddots & \vdots \\ nc_M^{(1)} & nc_M^{(2)} & \cdots & nc_M^{(T)} \end{bmatrix} \tag{2}$$

When both matrixes are multiplied with the vectors containing the weights that are given to each of the constraints, $\overline{\gamma} = [\gamma_1 \cdots \gamma_N]$ for the terminal and $\overline{\lambda} = [\lambda_1 \cdots \lambda_N]$ for the network and, furthermore, they are modulated by the parameters which provide a relative weight to each of the involved entities, the overall Selected Access (SA) is established, as shown in 3, which is just the matrix version of the expression previously presented.

$$\mathbf{SA} = \varGamma \ \left(\overline{\gamma} \cdot \mathbf{TC}\right) + \varLambda \ \left(\overline{\lambda} \cdot \mathbf{NC}\right) \tag{3}$$

The next step is therefore to sort the SA vector, selecting the element which has the higher value, provided that the corresponding base station has enough resources to satisfy the service. If such is not the case, the corresponding set is iterated, until an element able to handle the request is found.

As can be seen, the algorithm is generic and flexible enough and, thus, adding new constraints and/or modifying the weights given to the existing ones does not require relevant modifications.

3 Simulator Configuration

The scenario which will be used during the analysis entails a relatively large number of access alternatives, and we will assume that all terminals within the area of analysis are equipped with three radio access technologies (RAT) and, thus, they would be able to connect to any base station, provided that they are within their coverage area. In order to measure the different capacities which might be requested by the different services and to be able to assign resources accordingly, a generic capacity unit (*Traffic Unit, TU*) will be used during the analysis so as to characterize both the services requirements as well as the capacity of the different base stations. Table 1 summarizes the characteristics of the three RATs which have been employed during the analysis. As can be seen, both RAT-1 and RAT-3 aim at emulating the characteristics of typical WLAN technologies, while RAT-2 could be related with a legacy cellular access technology, with a much broader coverage area and higher capacity. We assume an ideal (i.e. disk-radius) channel model, although, as will be later explained, we modulate the *'link quality'* based on the distance between the end-user and the base station.

Table 1. Access technologies used during the access selection mechanism evaluation

RAT	**Coverage** (m)	**Number of Cells**	**Capacity per Cell** (TU)
1	80	30	5
2	600	4	30
3	60	20	5

Since there might be some end-users not willing to participate in the multi-hop extensions (this might impose, e.g. a higher energy consumption), we will assume that only half of them (i.e. 50% are relaying traffic); furthermore, considering the characteristics of the RATs they are equipped with, only RAT-1 is employed in the forwarding procedures. At the time of writing, the use of multi-hop communications with cellular technologies is far more difficult.

Nodes move according to the *Random Waypoint* mobility model within the area under analysis, which is assumed to be squared, with 1000 m side. In this sense, an end-user would select a random direction, a speed uniformly distributed between 2 and 3 m/s and a movement time, also uniform in the interval $[100, 120]$ s. Each time a node reaches the final destination of its current movement, it stays for a *pause* time at that position, also randomly selected in $[5, 10]$ s. Furthermore, whenever an end-user reaches any of the four edges of the simulation area, a reflection mechanism is applied, continuing its movement afterwards.

The last aspect which needs to be considered is the way nodes generate traffic. In order to better analyze the performance of the algorithms, we will assume a high load within the network. Traffic will be generated according to the *Poisson* model; each end-user can be seen as an independent traffic source, with two different services, which we assumed cannot be requested simultaneously. Table 2 shows the characteristics of these two services, where λ is the average number of calls per minute and μ^{-1} is the average duration of a call (in seconds).

Finally, we also need to identify which are the particular constraints which will be taken into consideration while building the SA. In the case of the end-user, two different aspects will be considered.

Table 2. Characteristics of the services used during the access selection algorithm evaluation

Service	λ (min^{-1})	μ^{-1} (s)	**Capacity** (TU)
1	0.6	120	1
2	0.6	80	3

- **Quality (tc_1).** It represents the quality of the link between the terminal and the Access Element. It is scaled, so as to always take a value between 0 and 1, thus emulating the information which shall be provided by an abstraction entity (which is a focal part of any access selection architecture, as it was discussed in Section 1). In this case, it is calculated from the relative distance to the base station (taking into account the particular coverage of the corresponding RAT), reaching the maximum value (1) when the position of the terminal is the same as the the base station one, and 0 when it is placed just at the coverage area border[1]. It is worth mentioning that, for the case

---

[1] We know that this is a simplification, but our goal is to have a bounded value between 0 and 1 for the sake of the proposed algorithm; introducing more realistic channel models would not have a strong impact, provided that this interval is respected.

of multi-hop routes, the lowest quality of the path has been taken at the overall quality of the access alternative, although this assumption can be easily adapted.
- **Handover (tc_2).** This parameter represents the preference that any end-user might have of keeping the communication with the current access and, whenever necessary of trying to prioritize those base stations which have the same technology as the currently active one. In order to reflect this, we use three different values for this parameter: $tc_2 = \{0, 0.5, 1\}$, whenever the current service is moved to a completely different base station, to an access alternative with the same RAT as the current one, or when it is not moved at all, respectively. This constraint aims at emulating the desire of the end-users to minimize the delay in which they incur during a handover procedure.

On the other hand, the network will certainly have other interests to look at, and the two following constraints will be applied.

- **Load (nc_1).** It might be the most relevant parameter from the perspective of the network when establishing the *Selected Accesses*. The goal is to balance the load of the different base stations, and therefore it uses the relative remaining capacity for each of them, so that when all resources are available, 1 is assigned to this parameter, while a 0 implies that a base station does not have any available capacity.
- **Handover (nc_1).** This constraint, which is pretty similar to the corresponding one at the terminal side, is used so as to model the interest that the network might have to maintain the connections at the same base stations as much as possible, so as not to incur in the cost associated to the handover procedures. It will use the same values as the ones which were established for the terminal.

4 Discussion of Results

The main goal of this first study is to analyze different combinations of the corresponding weights, so as to allow us establishing their best configuration. Afterwards, these combinations could be challenged over different scenarios (increased number of users, different setup of Access Elements, etc). Hence, we do not assume any *prior* assumption about the values which the weights should have, rather we aim at finding sensible choices for them.

The following parameters will be analyzed.

- **Reject probability.** It refers to those requests which were not handled by the network.
- **Anomalous termination.** It considers those calls that, albeit having started correctly, did not end properly, due to the fact that there were not available resources on the potential new base stations during a handover process to satisfy their capacity needs.

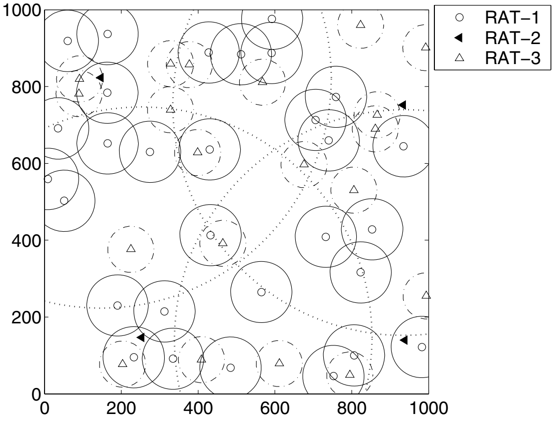


Fig. 2. Base station deployment

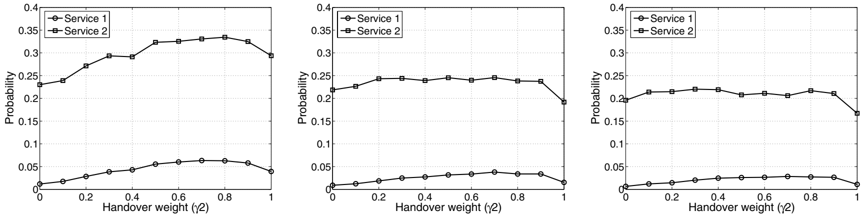
- **Average number of handovers per service.** We will differentiate between those involving base stations of the same RAT (Intra-RAT) as well as those which happen between different RATs (Inter-RAT).
- **Relative load.** This parameter allows analyzing how well the load was distributed between the different network Access Elements, since it is defined as the relative available capacity.
- **Overall network load.** It can be used so as to study the performance (or throughput) which can be obtained, by using the different access selection strategies.

In all cases, we have used the same network deployment, in which the base stations were randomly deployed (ensuring a minimum distance between two of the same kind). The particular deployment which was used (shown in Figure 2) ensures enough overlapping, while the four RAT-2 base stations cover the whole simulation area. Each of the scenarios is simulated 20 times, presenting the average results, so as to ensure tight confidence intervals.

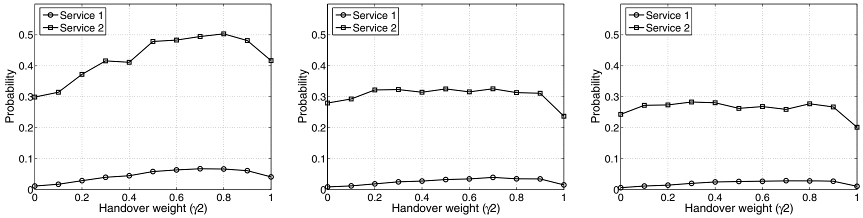
4.1 Terminal Centric Strategy

In this case, we assume that it is the terminal the entity with the overall responsibility when deciding on the Access Element to connect to, and thus $\Gamma = 1$ and $\Lambda = 0$. Under these circumstances, we will study the influence of using different weight combinations (γ_i). Since we are using only two parameters and $\sum_i \gamma_i = 1$, we can yield that $\gamma_1 = 1 - \gamma_2$.

Figure 3 shows both the reject probability and the percentage of calls that did not end properly. We can see that both of them are much more relevant for the second service, due to the fact that it requires a higher capacity. We can also see that there is not a remarkable influence of the particular configuration of the weights, since the probabilities are almost stable for the various values of γ_i



(a) 1 hop (b) 2 hops (c) 3 hops

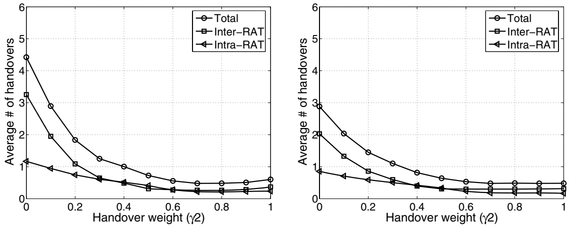


(d) 1 hop (e) 2 hops (f) 3 hops

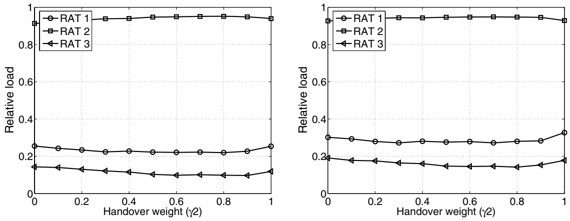
Fig. 3. Reject (top) and anomalous termination (bottom) probabilities with the *Terminal Centric* strategy

which have been used. Last, but not least, multi-hop extensions bring about an important improvement from the point of view of the *quality of service* perceived by the end-users, as both probabilities decreases as we augment the maximum number of hops which can be used to reach a base station (around 10 % for the reject probability a and almost 20 % for the anomalous termination); we also see that this influence is less relevant when going from 2 to 3 hops (close to 5 % for both parameters).

Figure 4 shows the average number of handovers per service and the relative load per RAT. From the point of view of the handover events, it is clear that as long as we increase γ_2 (weight given by the terminals to the constraint of maintaining the same base station), the average number of handovers decreases. There is a slight change of tendency close to $\gamma_2 = 1$, which is due to the fact that in this case there will be more connections with a poor quality (close to the cell border, which eventually will require a handover soon. In this case we only present the results which were obtained for a single-hop, since there was not much difference for the other two configurations. We see that the number of handovers for the second service is lower, which could have been expected, since the average duration of this service is shorter. Regarding the relative load, the first thing to highlight is that RAT-2 base stations are the more loaded ones, since their coverage is much broader than the other two. When we increase the number of hops we can see how the load is better balanced, since thanks to the multi-hop routes there might be more chances to reach one of the base stations with RAT-1 or RAT-2 (around 10 % increase).



(a) Service 1 (b) Service 2



(c) 1 hop (d) 2 hops

Fig. 4. Average number of handovers (top) and load balancing (bottom) with the *Terminal Centric* strategy

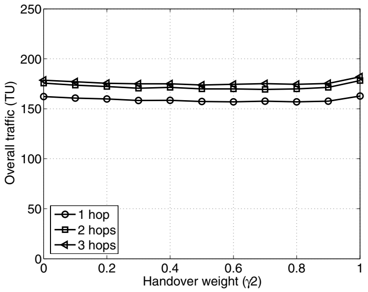
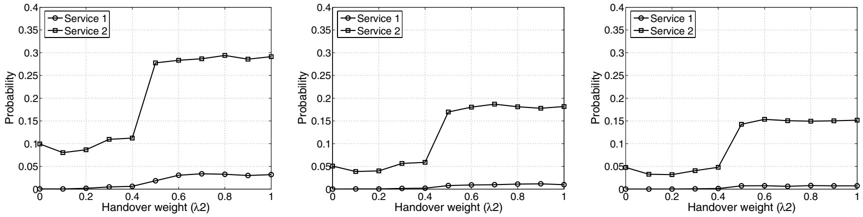


Fig. 5. Overall network throughput with the *Terminal Centric* strategy

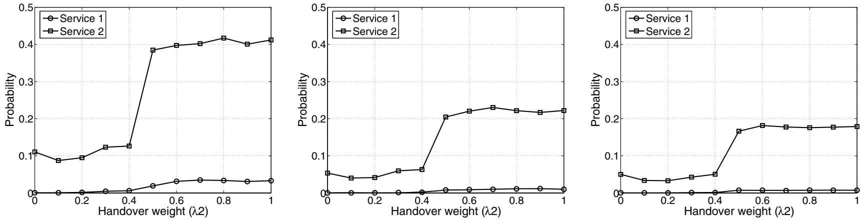
Finally, Figure 5 shows that the overall network performance increases when we enable the multi-hop extensions. This is a very relevant result, since it yields an additional benefit of multi-hop topologies, from the point of view of the operators. Traditionally, most of the benefits of the these network extensions (enhanced coverage, better performance) were more closely related to the end-user, but Figure shows that the operator would also obtain benefit from them.

4.2 Network Centric

In this case, we give all the responsibility of the decision process to the network and thus, Λ takes a value of 1, and Γ is 0. Under these circumstances, we analyze



(a) 1 hop (b) 2 hops (c) 3 hops



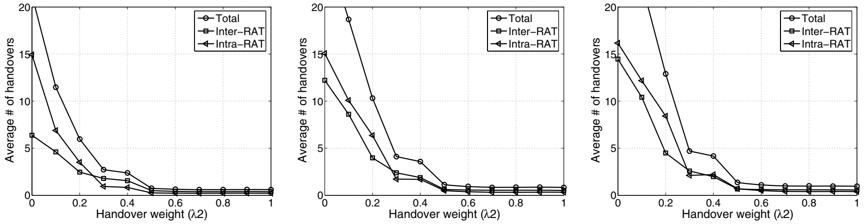
(d) 1 hop (e) 2 hops (f) 3 hops

Fig. 6. Reject (top) and anomalous termination (bottom) probabilities with the *Network Centric* strategy

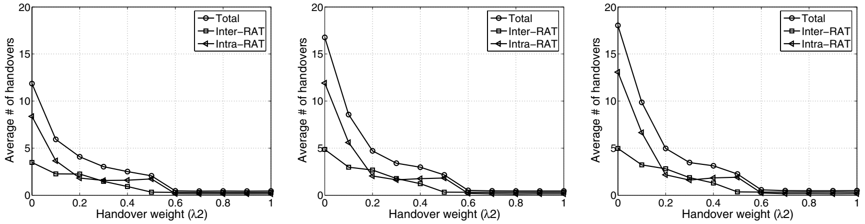
which is the consequence of tweaking the access selection strategy, by varying the weight of the two constraints, λ_i; again, it is clear that $\lambda_1 = 1 - \lambda_2$.

Figure 6 shows the reject and anomalous termination probabilities; in this case we can also see the benefits of the multi-hop extensions, since both probabilities are heavily reduced when increasing the maximum number of hops which can be used to reach a base station (10 % and 20 %, respectively, when increasing from 1 to 2 hops, and $\tilde{5}$ % when allowing up to three hops). For instance, we can see that both probabilities almost reaches 0 for the first service when three hops are allowed to reach an Access Element. Besides, the effect of the multi-hop extensions are more clear in this case; this is a direct consequence of the load balancing procedure which is used by the base stations, which maintains a bunch of available resources in the network. In fact, this improvement is even more remarkable, when we increase the weight given to the load balancing constraint. Finally, and opposed to the Terminal Centric approach, the figures show that there is a strong influence on the particular configuration of the access selection strategy (values λ_1 and λ_2) in the obtained results. In all the analyzed cases, we can clearly distinguish two areas, with a relevant penalization on the QoS perceived by the end-users when λ_2 is higher than 0.4; however, both metrics stay quite stable in the two resulting intervals.

On the other hand, Figure 7 shows the average number of handovers which are executed per service for the different configurations of the *Network Centric* strategy. The first aspect to be highlighted is the values obtained for the lowest values of λ_2, for which we can see a high number of handovers taking place. The reason behind this aspect is that, in these circumstances, the main (and almost



(a) 1 hop - Service 1 (b) 2 hops - Service 1 (c) 3 hops - Service 1



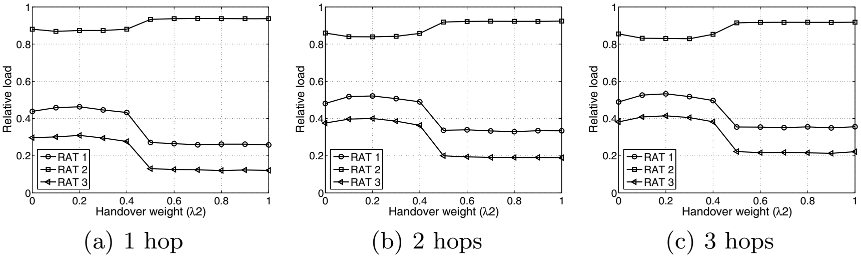
(d) 1 hop - Service 2 (e) 2 hops - Service 2 (f) 3 hops - Service 2

Fig. 7. Average number of handovers for the *Network Centric* strategy

unique) goal of the access selection strategy is to balance the load between all the base stations, and thus it is sensible thinking that there might be some *ping-pong* effect, shifting the communications between base stations almost continually. As soon as the weight that the network gives to keeping the calls on the same base station takes a sufficiently large value (0.4), the number of handovers heavily decreases and, from that moment, it is maintained on a reasonably low values, independently of the configuration of the access selection strategy. Regarding the influence of the maximum number of hops which can be used, we perceive a light increase of the average number of handovers when increasing route lengths, but the difference is almost negligible for values of λ_2 higher than 0.4, as it was also observed for the *Terminal Centric* strategy.

Taking into account that this was one of the main objectives of the *Network Centric* access selection strategy, the values which are observed in Figure 8, which shows the relative load per RAT, could have been anticipated. In this case, traffic is much fairer distributed between the different types of base stations which conform the scenario under analysis. The two previously identified intervals are again easily identified in the figures, being the boundary once more around $\lambda_2 = 0.4$, as it happened with the previously studied parameters. However, the aspect which more clearly appears this time is that the effect of increasing the number of hops which can be used to reach a base station has a strong influence, as we can see a notable enhancement of the occupancy of both RAT-1 and RAT-3, especially when we increase from one to two hops (around 10 %).

Finally, Figure 9 shows the improvement from the point of view of the overall network throughput. Again, we see that the multi-hop extensions can provide a



(a) 1 hop (b) 2 hops (c) 3 hops

Fig. 8. Relative RAT load with the *Network Centric* strategy

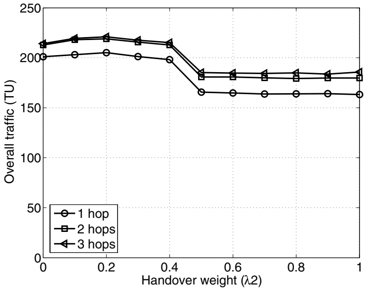


Fig. 9. Overall network throughput with the *Network Centric* strategy

significant revenue increase to the operators and that, in this case, the overall throughput is higher than in the *Terminal Centric* strategy, as could have been expected, since the goal of the network should be to maximize the overall load.

5 Conclusions

By using a generic access selection algorithm we have evaluated the performance of different access selection strategies. We have analyzed two complementary approaches, one centered at the end-user terminal and the other one centered at the network. For the two of them, different configurations, based on various parameters, have been used. The obtained results could help to establish an optimum configuration for the access selection strategy.

Furthermore, we have seen that the use of multi-hop extensions may bring about different benefits, not only to the end-users, but also to network operators, since they will facilitate an increase on the overall network throughput.

In the future we will analyze other access selection strategies, combining the preferences of the terminals and the network, as well as adding more constraints into the picture. In addition, we will compare the results by running the access selection algorithm with the optimum values, using Optimization Techniques to find these benchmarks.

Another item which is left for future work is to account for more realistic channel models, according to the specific considered technology and to analyze the drawbacks of the multi-hop extensions (e.g interference).

Acknowledgements

The authors would like to express their gratitude to the Spanish government for its funding in the following two projects: Mobilia - CELTIC Program (Avanza I+D TSI-020400-2008-82) and "Cognitive, Cooperative Communications and autonomous SErvice Management", C3SEM (TEC2009-14598-C02-01).

References

1. Sachs, J., Agüero, R., Daoud, K., Gebert, J., Koudouridis, G.P., Meago, F., Prytz, M., Rinta-aho, T., Tang, H.: Generic Abstraction of Access Performance and Resources for Multi-Radio Access Management. In: Advances in Mobile and Wireless Communications. Springer, Heidelberg (2008)
2. Sachs, J., Prytz, M., Gebert, J.: Multi-access Management in Heterogeneous Networks. Wireless Personal Communications 48(1) (2009)
3. Dimou, K., Agüero, R., Bortnik, M., Karimi, R., Koudouridis, G.P., Kaminski, S., Lederer, H., Sachs, J.: Generic link layer: a solution for multi-radio transmission diversity in communication networks beyond 3G. In: Proceedings of Vehicular Technology Conference (VTC fall 2005), Dallas, USA (2005)
4. Sooriyabandara, M., Farnham, T., Efthymiou, C., Wellens, M., Riihijärvi, J., Mähönen, P., Gefflaut, A., Galache, J., Melpignano, D., Van Rooijen, A.: Unified Link Layer API: A generic and open API to manage wireless media access. Computer Communications 31(5) (2008)
5. Mäkelä, J., Pentikousis, K.: Trigger management mechanisms. In: Proc. of the Second International Symposium on Wireless Pervasive Computing (ISWPC), San Juan, Puerto Rico, USA (2007)
6. Magnusson, P., Berggren, F., Karla, I., Litjens, R., Meago, F., Haitao, H., Veronesi, R.: Multi-radio resource management for communication networks beyond 3G. In: VTC Fall 2005 IEEE 62nd Semiannual Vehicular Technology Conference on, vol. 3, pp. 1653–1657 (2005)
7. Johnson, M., Sachs, J., Rinta-aho, T., Jokikyyny, T.: Ambient Networks - A framework for multi-access control in heterogeneous networks. In: Proc. IEEE 64th Vehicular Technology Conference (VTC Fall 2006), Montreal, Canada (2006)
8. Perez-Romero, J., Sallent, O., Agusti, R., Karlsson, P., Barbaresi, A., Wang, L., Casadevall, F., Dohler, M., Gonzalez, H., Cabral-Pinto, F.: Common Radio Resource Management: Functional Models and Implementation Requirements. In: Proc. of PIMRC 2005, Berlin, Alemania (2005)
9. Olmos, J., Ferrús, R., Sallent, O., Pérez-Romero, J., Casadevall, F.: A Functional End-to-End QoS Architecture Enabling Radio and IP Transport Coordination. In: Proc. of IEEE WCNC (2007)
10. Pentikousis, K., Agüero, R., Gebert, J., Galache, J., Blume, O., Paakkonen, P.: The Ambient Networks Heterogeneous Access Selection Architecture. In: Proc. of the First Ambient Networks Workshop on Mobility, Multiaccess, and Network Management (M2NM 2007), Sidney, Australia (2007)

11. Salkintzis, A.: Interworking Techniques and Architectures for WLAN/3G Integration Toward 4G Mobile Data Networks. IEEE Wireless Communications, 50–61 (June 2004)
12. Ma, L., Yu, F., Leung, V., Randhawa, T.: A New Method to Support UMTS/WLAN Vertical Handover Using SCTP. IEEE Wireless Communications, 44–51 (2004)
13. Wu, W., Banerjee, N., Basu, K., Das, S.K.: SIP-Based Vertical Handoff between WWANs and WLANs. IEEE Wireless Communications, 66–72 (2005)
14. Berggren, F., Litjens, R.: Performance analysis of access selection and transmit diversity in multi-access networks. In: Proc. 12th Annual International Conference on Mobile Computing and Networking, pp. 251–261 (2006)
15. Olmos, J., Ferrús, R., Sallent, O., Pérez-Romero, J., Casadevall, F.: A Functional End-to-End QoS Architecture Enabling Radio and IP Transport Coordination. In: Proc. of the First Ambient Networks Workshop on Mobility, Multiaccess, and Network Management (M2NM 2007), Sidney, Australia (2007)
16. Mobility Concetps for IMT-Advanced (Mobilia) Project; BWA and 3G requirements for heterogeneous access and service framework architecture, D4.1 (2009)
17. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution: Report on Technical options and Conclusions (Release 7), TS23.882v160 (2006)
18. Niyato, D., Hossain, E.: A Game Theoretic analysis of service competition and pricing in heterogeneous wireless access networks. IEEE Transactions on Wireless Communications 7(12) (2008)

Experimental System Level Platform for B3G Scenarios

V. Monteiro[1], J. Bastos[1], O. Cabral[2], F. Velez[2], and J. Rodriguez[1]

[1] Instituto de Telecomunicações, University of Aveiro,
Campus de Santiago, 3810-094 Aveiro, Portugal
`{vmonteiro,jbastos,jonathan}@av.it.pt`
[2] Instituto de Telecomunicações, DEM, Universidade da Beira Interior,
6201-001 Covilhã, Portugal
`{orlandoc,fjv}@ubi.pt`

Abstract. This paper provides a complete specification of the packet based cellular wireless system level simulator that addresses a beyond 3G scenario involving heterogeneous wireless systems interconnected via an IP backbone network. Important aspects as the Link layer design (including the MAC layer) are specified, as well as the C++ object oriented simulation architecture. Since the IP level and the physical layer aspects should be avoided, interfaces representing these layers are proposed for different type of radio access systems. The concept is showcased by a multi-RAT system composed of HSDPA and a Wi-Fi system using load balancing techniques.

Keywords: Cross-system, simulation, multi-RAT, beyond 3G.

1 Introduction

The rapid evolution of Internet services and increasing interest in portable computing devices are likely to create large demands for high-speed wireless data services. Especially in the downlink, high throughput is needed since the number of multimedia applications and downloads of large data files from web sites and servers are increasing. To address this future requirement Beyond 3rd Generation (B3G) systems will provide mobile ubiquitous connectivity at any time. This raises significant research challenges in the way legacy and future emerging systems need to coexist and specifically "cooperate" to ensure spectral resources are efficiently exploited in an era where radio spectrum is at a premium.

Efficient use of radio resources requires Cooperative Radio Resource Management (CRRM), a module that carries out RRM on a global scale between system of diverse technologies and operators. To solve the CRRM challenge, an experimental platform is required that models all environmental and system issues pertaining to a heterogeneous networking scenario, and that has desirable attributes that include: low complexity and simulation time and high modeling accuracy.

This paper presents an experimental system level platform for validating cooperative RRM algorithms in B3G scenarios based on IP traffic, using wireless systems like HSDPA and Wi-Fi. The rest of this paper is organized as follows. Section 2 addresses the system level simulator architecture based on a layered structure of communication systems. Section 3 presents an example of utilization of such a simulator

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 57–67, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

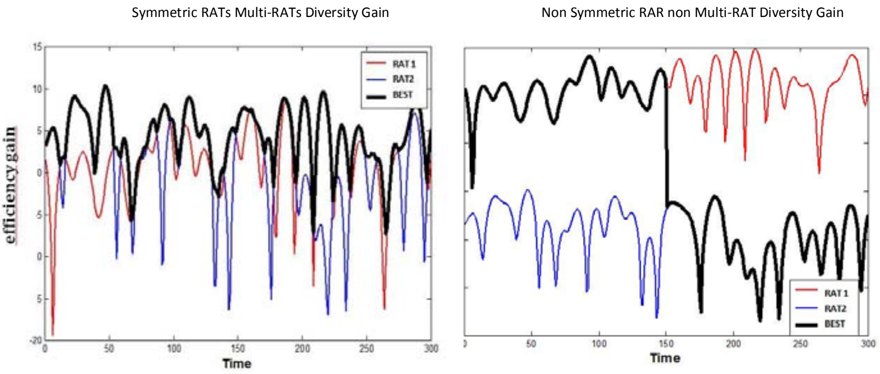
in a scenario with a multi-RAT (Radio Access Technology) system composed by the UMTS HSDPA and the mobile Wi-Fi. Besides the simulation scenario description performance results are presented. The conclusions are drawn in Section 4.

2 System Level Simulator Architecture

2.1 Multi-RAT Diversity

A heterogeneous wireless environment demands significant upgrades to the existing communication paradigm in terms of infrastructure, devices and services to support the *anytime*, *anywhere*, *any-technology* and *any-standard* philosophy. These changes introduce novel and fast-evolving requirements and expectations on research and development in the field of information and communication technologies.

Figure 1 presents the idea of multi-RAT diversity. As it can be seen on the left plot, the selected RAT is always the most efficient one, enabling to achieve the multi-RAT diversity gain. Besides, the selected RAT varies according to a certain period. Although fairness is taken into account, the diversity gain is not exploited. Exploiting the multi-RAT diversity and applying fairness, i.e., maintaining QoS and delay levels, is one of the most interesting challenges in packet based wireless cellular systems. This trade-off between promoting fairness and maximizing system capacity is typically controlled by the scheduling policy.


Symmetric RATs Multi-RATs Diversity Gain

Non Symmetric RAR non Multi-RAT Diversity Gain

Fig. 1. Multi-RAT diversity concept

2.2 Problem Domain

In order to reflect a realistic system, the performance evaluation should consider the impact of the relevant layers of the communication protocol: physical layer, link-layer (L2 layer) and upper layers. The details of the Link Level Interface to the Physical layer can be found in [1]. The structure of a single RAT simulator for the HSDPA case, with some of the blocks describing the functions described above, is presented in Figure 2.

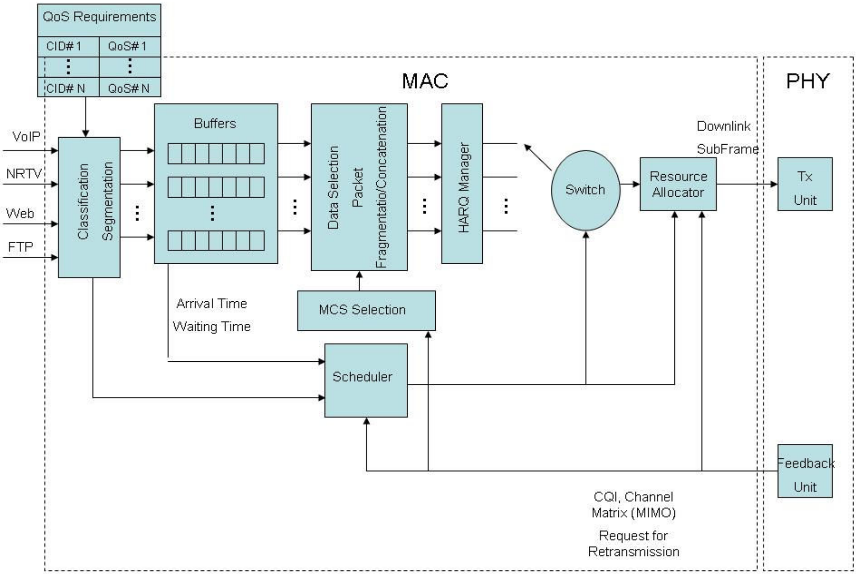


Fig. 2. Simulator structure for one RAT (HSDPA case)

The MAC layer includes two types of models: MAC protocols that include algorithms and procedures which affects the system performance and optimization, such as Call Admission Control (CAC), Handover, Dynamic Channel Allocation; and the other group related to the modeling of the system in order to validate the MAC protocol/algorithms, such as mobility models, service models and traffic queues, radio channel propagation model and physical simulation area. More specifically, the MAC components include:

A) MAC protocols

Scheduling. The scheduler decides how to allocate the appropriate radio resources to each user based on the following context information: service type, user QoS profile, and channel performance. In WCDMA, four types of scheduling are defined:

- Time division scheduling: This is based on the concept of several users sharing the same transport channel in the time domain. Thus each user will be allocated the entire bandwidth for a short period of time, each sharing the same code. This technique provides code efficiency, and is more suitable for bursty traffic. In addition, it can provide appropriate link performance due to the high data rate. This scheme is usually used with shared channels. This type of allocation will provide high interference variations with time, thus having impact on real time services.
- Code division scheduling: Each user is given bandwidth on demand, by allocating the users with different codes. The scheme is associated with dedicated channels, and low bit rate users. It will provide an initial delay on set-up, and can lead to more predictable interference loading. The efficiency of this type of scheduling

depends on the accurate estimate of the average bit rate. A poor estimate will lead to inefficient use of the spectrum, thus a dynamic allocation scheme is desirable.
- Power based scheduling: It allocates resources based on the user location, assigning low bit rates to users near the cell edge, and higher bit rates to those nearer the base station. This scheme will have direct improvement on the average downlink capacity.
- Sub-channel based scheduling: This is a specific scheme for Orthogonal Frequency Division Multiple Access (OFDMA) systems. Allocation is performed on the basis of sub-channels. A number of sub-channels is allocated per used as a function of the fading affecting these bands. The achieved improvement is in terms of bandwidth required by the user application while optimizing band utilization.

Although all the schemes can provide performance improvements in different conditions, there is no single scheme that can be considered to be the best candidate. Typically, combinations of scheduling techniques are used to provide overall performance gain. In this paper, the scheduler is based on time division although it can be extended to consider allocating resources both in time and frequency. Still, only dedicated transport channels will be considered in the reference stage, and channel signaling time set-up will be implicitly assumed, but will not be considered in the overall delay associated with dropping a packet session.

In HSDPA, scheduling refers both to selecting packets based on priorities primitives, and mapping them into resources (time slots, coding and carriers), using cross-system information whose content is delay requirements for the service (from upper layer) and suitable slot/carrier for this service.

Automatic Repeat Request. Simple Automatic Repeat Request (ARQ) will be employed for non-real time services. It is assumed that variable IP packet sizes are translated to fixed packet sizes in the Radio Link Control (RLC) layer, through segmentation, concatenation and padding. When the link quality is below the target level, the QoS block will decide whether to drop any packets based on the average Signal-to-Interference Ratio (SIR) value measurement and target value. Packets that are assumed to arrive with error will be dropped and retransmitted. The retransmission is implicitly assumed, and the delay counter associated with the user queue will be incremented accordingly. We assume that many packets can arrive within the time interval. If the SIR is below the target value, a Packet Error Ratio (PER) model will suggest whether the specific packet is in error.

B) System models

Mobility models. Typical models are being employed to model mobile movement in indoor, outdoor urban, and sub-urban environments. Parameters associated with mobility include speed, probability to change speed at position update, probability to change direction, and the de-correlation length. The latter will dictate the simulator time interval between mobility updates. A detailed specification is given in [2].

A simulator map provides a description of the cellular map, which includes the cell descriptions, base station locations, and the manner in which it will model mobile movement at the system boundaries. A wrap around model is being used, instead of modeling mobile movement bouncing of the edges of the outer-cells. This means that the mobile may migrate off the edge of the system boundary and, emerge on the opposite side, in a wrap around fashion.

QoS measure. This module is responsible for analyzing the link quality for each transport channel. If the quality deteriorates below a certain level, then it will take the appropriate action. It will increment the service delay counter, and will drop the packet session if the maximum delay has been exceeded. The detailed definition of the dropping criteria is given in [2] [3] and [4].

Service Queue. All services are packet based, and defined by the QoS context, that will include information such as instantaneous bit rate, average bit rate and current delay, and maximum tolerated delay. All new incoming users will be assigned a priority value, and then placed in the queue. This service queue will list all the mobiles that are waiting to be served, as well as all users that have already been allocated a transport channel. The QoS Control block will look at this table to check whether any user has breached the QoS, and drop it from the system.

Dynamic Channel Allocation (DCA). The DCA algorithm is considered since it provides extra performance tracking the channel variations. It is important to validate the basic simulator architecture at the earliest design stage, and to provide some benchmark performance curves. In this way, the immediate improvement given by DCA can be noticed at the intermediate design stage, and verified. The need for DCA arises when changes either in the traffic, or channel conditions lead to under occupancy and a reduction in the QoS.

Propagation Module. The module will model path loss and slow fading. Channel models for indoor environments, outdoor urban and rural environments will be provided.

Link Level Interface. To provide an adaptive solution, the system level platform must be integrated into the Link Level platform. This solution is not efficient, and there is a direct trade-off between modeling accuracy, complexity and simulation time. Therefore, the PHY layer is typically modeled by a Link Level Interface in the form of look-up tables, that models the average link performance for a given scenario defined by the channel, interference models, mobility and service. Moreover, an interface translates the system level parameters into the appropriate transport format parameters to simulate the Link Level chain, resulting in a table with SIR vs. PER (Packet Error Rate) for a specific simulation environment.

Mobiles. The system will have the flexibility to support different mobile types, supported by the inheritance attribute C++ offers. Each mobile type will be defined by the following parameters:

- Antenna type: antenna type will be assumed to be omnidirectional;
- Maximum transit power: the maximum transmit power the mobile can support;
- Mobile noise figure: the receiver sensitivity;
- Power dynamic: the transmit power range the mobile can support between a maximum and a minimum;

- Mobile coordinate: each mobile is responsible for updating its coordinates, in terms of position and velocity.

In the reference stage, it is assumed that the same mobile type is considered for all the scenarios.

Base Station/APs. As in the mobile case, the Base Station class is a template, which will support child objects with added functionality. This generic template can be defined as:

- Antenna type: antenna type will be assumed to be omnidirectional;
- Maximum transit power: the maximum transmit power the mobile can support;
- Base Station noise figure: the receiver sensitivity;
- Power dynamic: the transmit power range the mobile can support between maximum and minimum;
- Resource Unit Identifier: A 3-D coordinate provides a description
- of the frequency slot, time slot, and code number.

Signaling: All signaling is implicitly modeled to reduce simulator processing overhead.

Transport Channels. Transport channels reflect the available resources in the cell. Separate resources exist for both uplink and downlink. The capacity of the resource unit is dependent on the receiver and frame structure, as well as on channel link quality.

The structure of the simulator with some of the blocks describing the functions described above is presented in Figure 2.

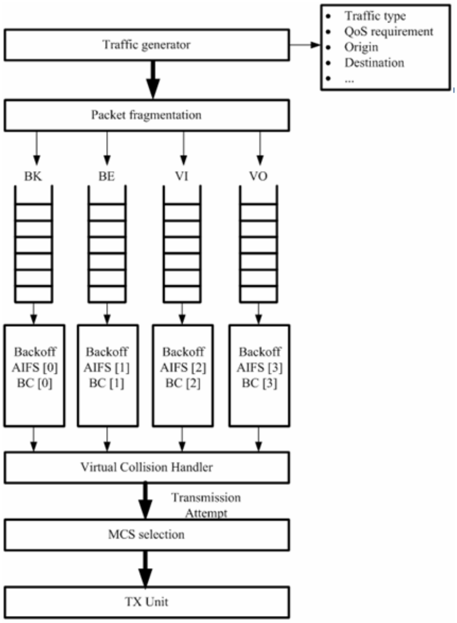


Fig. 3. Structure for decentralized based RATs (Wi-Fi case)

2.3 Extension of Simulation Structure for Distributed Systems

Previous section presented a simulator structure for centralized systems, where HSDPA is included. Figure 3 presents the main blocks for the Wi-Fi (IEEE 802.11e) case which a distributed system. As distributed (Wi-Fi) and centralized (HSDPA) systems are very different systems in terms of main control, we will need a collision handler block in the 802.11 case. While in HSDPA, as it is a centralized system, there is one main controller that does the scheduling, the resource allocation, etc., in Wi-Fi, as it is a decentralized system all the entities/machines in the scenario follow the structure in Figure 3. More details on the Wi-Fi simulator design can be found in [5].

3 Simulation Showcase

In this section we present a practical example of utilization of the proposed modeling approaches for co-existence system level simulations. In the simulation showcase we evaluate the application of cooperative RRM in term of QoS performance for underlying radio access systems that includes interoperability between Release 5 of HSDPA and IEEE 802.11e (Wi-Fi).

3.1 Load Balancing

A load balancing algorithm that aims to optimize the spectral efficiency in the co-existence scenario is presented herein. The algorithm is based on service suitability [6] which aims to allocate new users to the most suited radio access networks according to the application at hand. The algorithm calculates a suitability value *S*, and is expressed by the following equation

$$S(L(cell_{i,j})) = \begin{cases} 1 & if \quad L(cell_{i,j}) \le LTh_j \\ \left(\dfrac{1 - L(cell_{i,j})}{1 - LTh_j} \right)^2 & if \; L(cell_{i,j}) > LTh_j \end{cases} \tag{1}$$

and depicted graphically in Figure 4, where $cell_{i,j}$ represents the cell or access point i belonging to the RAT j, $L(cell_{i,j})$ is the normalized load in the $cell_{i,j}$, LTh_j is the load threshold for RAT j, and $S(L(cell_{i,j}))$ is the suitability value for accepting a new user in the $cell_{i,j}$. LTh_j is the parameter of the algorithm and characterizes the amount of load reserved for preferable traffic; the latter is a variable that must be optimized by the operator to set the amount of traffic that a RAT will use for preferable services.

3.2 Simulation Scenario

The simulation scenario envisages mobiles that are created at the beginning of each simulation run, and remain active for the complete duration. Furthermore, the path loss and shadowing values remain constant within a run, whilst the fast fading is updated on each Transmission Time Interval (TTI) [7]. Simulations were conducted in an indoor environment where each run corresponds to 300 seconds real time, and each TTI is 2 ms. The traffic model follows 3GPP proposed models [8] and the RATs are selected according to their load. The simulation parameters are presented in Table 1.

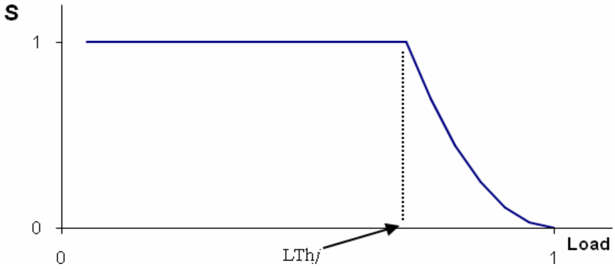


Fig. 4. Suitability for the load balancing selection algorithm

3.3 Simulation Results

Two measures were defined to analyze system performance: QoS and Service throughputs. Service throughput is the number of bits that have been transmitted and correctly received in the cell, during the simulation, divided by the total simulation duration. QoS throughput is the number of bits correctly received within the allowed delay during the simulation, divided by the total simulation duration.

The outage probabilities of the QoS and Service throughputs are compared in Figure 5 for the HSDPA system alone. It can be seen that the outage probability for QoS throughput is stable with the offered load until the HSDPA system capacity is reached (with about 30 users). As the offered load (number of users) goes beyond this value, the outage probability for the QoS and Service throughputs expectedly drops. QoS throughput drops faster than the service throughput as it accounts not only for the packets that are correctly delivered, but also for the packets that are delivered within a given delay threshold.

Table 1. Simulation parameters for the indoor scenario

Simulation parameters	HSDPA (Rel.5)	Wi-Fi (802.11e)
Scenario Deployment		
Cell type	Omni	Omni
Cell radius	50 m	35 m
Mobiles velocity	3km/h	3km/h
Path loss and shadowing	3GPP indoor channel	ITU for the 2GHz band
Fast fading component	ETSI Indoor A	Not used
Services		
Near Real-Time Video	[8]	[8]
Dynamic Resource Allocation		
Scheduler	Max C/I	EDCA mode
Link Adaptation criteria	$CQI = Max(\arg_{CQI}(BLER(CQI) \leq 0.1))$	
H-ARQ type II	Asynchronous transmission with Chase Combining	
Link Level Interface	LUTs for 3GPP release 5 CQI using actual value interface methodology	

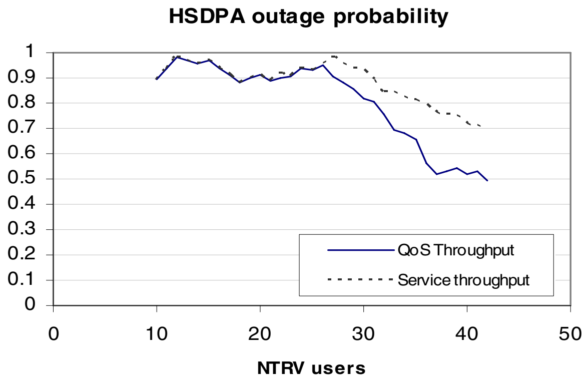


Fig. 5. Throughput results for standalone HSDPA system

Figure 6 presents results for Wi-Fi RAT alone. It can be noticed that the outage probability stays roughly constant for as much as 50 Near Real Time Video (NRTV) users. As Wi-Fi is a wideband system, it has enough room to fit all the NRTV users.

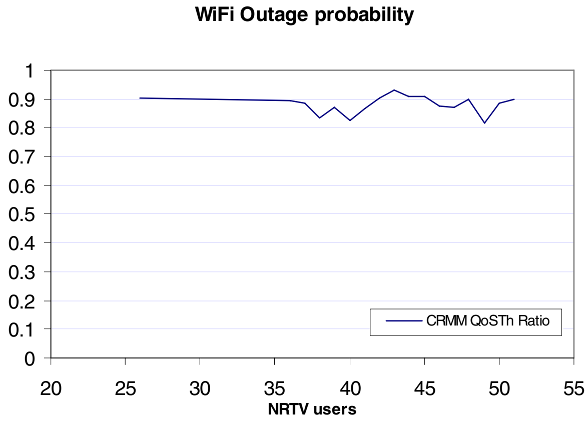


Fig. 6. IEEE 802.11e outage probability results

The application of cooperative RRM based on equation (1) in heterogeneous wireless systems is shown in Figure 7. In this specific case, we compare the performance using service suitability assuming underlying Wi-Fi and HSDPA systems, and the HSDPA standalone scenario. Results show that up to 100% of the 42 users can be supported when using CRRM in contrast to 60% users in the stand alone case, resulting in a gain of 40% in the outage probability. The gain comes from balancing and sharing resources from both bands and managing them as one where handovers between systems is completely transparent to the users.

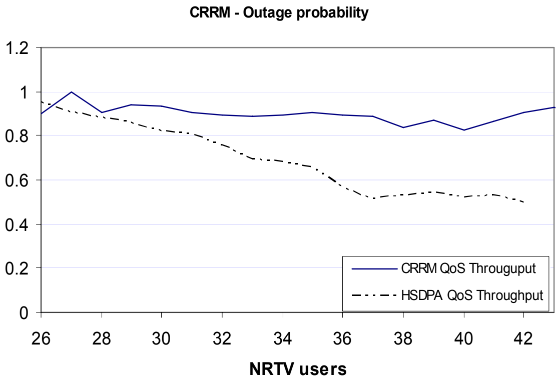


Fig. 7. Percentage of satisfied users using CRRM entity *versus* satisfied users using HSDPA alone

4 Conclusions

In this paper, a complete specification of a reference system simulator envisaged for packet based beyond 3G wireless systems, including modeling approaches for the IP layer, and Physical layer was presented. Furthermore, this paper validates the models using CRRM algorithm based on service suitability. The simulation showcase compared the performance using service suitability assuming underlying IEEE 802.11e and HSDPA systems, in contrast to the HSDPA standalone case. Results showed that up to 100% users can be supported when using CRRM in comparison to 60% users in the standalone case, resulting in a gain of 40% on outage probability.

Acknowledgements

This work has been performed in the framework of the MOBILIA project (CP5-016) under the Eureka Celtic Framework, the FCT PhD grant SFRH/BD/28517/2006, as well as the ICT projects ICT-217033 WHERE and ICT-248894 WHERE2, which are partly funded by the European Union. It was also partially funded by CROSSNET (Portuguese Foundation for Science and Technology, FCT, POSC project with FEDER funding), IST-UNITE, Fundação Calouste Gulbenkian, and ”Projecto de Re-equipamento Cientfico” REEQ/1201/EEI/2005 (a Portuguese Foundation for Science and Technology project).

References

1. Monteiro, V., Rodriguez, J., Nascimento, A., Gameiro, A.: Packet based system level simulator for cellular wireless B3G networks. In: Proc. of SIMUTools 2008, Marseille, France (March 2008)

2. ETSI: Universal Mobile Telecommunication System (UMTS); Selection procedures for the choice of radio transmission technologies of the UMTS (UMTS 30.03 version 3.2.0), TR 101 112 v3.2.0 (April 1998)
3. Holma, H., Toskala, A.: WCDMA for UMTS, 3rd edn. John Wiley & Sons, Ltd., England (2004)
4. 3GPP: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; QoS Concept and Architecture (Release 5), 3GPP TS 23.107 v5.5.0 (2002-2006)
5. Cabral, O., Segarra, A., Velez, F.J.: Event-Driven Simulation for IEEE 802.11e Optimization. IAENG International Journal of Computer Science 35(1), 161–173 (2008)
6. Rodriguez, J., Monteiro, V., Bastos, J., Gameiro, A., Cabral, O., Velez, F.: Service Suitability Based RAT Selection for Beyond 3G Systems. In: Proc. of VTC2008-Fall, Calgary, Canada, September 21-24 (2008)
7. Phan Huy, D.T., Monteiro, V., Gameiro, A., Rodriguez, J.: System level performance evaluation of MATRICE air interface. In: Proc. of IST Summit, Lyon, France (June 2004)
8. 3GPP TSG-RAN 1, Ericsson: System Level Evaluation of OFDM – further considerations, Document R1-03-1303, Lisbon, Portugal (November 2003)

TCP-Aware Forward Error Correction for Wireless Networks

Dzmitry Kliazovich, Magda Bendazzoli, and Fabrizio Granelli

DISI - University of Trento
Via Sommarive 14, I-38050 Trento, Italy
`{kliazovich,granelli}@disi.unitn.it,`
`bendazzoli@telefin.it`

Abstract. This paper studies TCP performance improvement in wireless and heterogeneous networks using Forward Error Correction (FEC) technique driven by TCP semantics. In the proposed scheme, called TCP-aware FEC, the amount of redundancy added to a packet at the sender node corresponds to the level of error protection and is computed as a function of TCP congestion window. The TCP-aware FEC becomes stronger for low congestion window values (experienced after a packet loss is detected), while the amount of added redundancy is reduced for the large window values approaching the capacity of the end-to-end link.

The design of TCP-aware FEC adaptability is driven by the mechanics of TCP congestion and flow control mechanisms, and it is based on the notion that link losses become more dangerous when congestion window and sending rate are low.

The proposed FEC scheme can be implemented either end-to-end as a part of TCP sender and receiver protocol stacks, or locally, covering the wireless part of the connection only. The performance results obtained through simulations confirm the design assumptions and underline the benefits of the proposed approach with respect to traditional FEC schemes[1].

Keywords: Adaptive FEC, TCP-aware.

1 Introduction

TCP is de facto standard protocol for communications in Internet [1]. Most of today's applications (including web access, file transfer, email, and even video streaming) demand TCP, mainly for its two major properties: reliable data delivery and congestion control. However, being designed almost 40 years ago for wired networks, TCP/IP reference model fails to deliver sustainable performance in heterogeneous network environments, which often includes wireless links [2].

Wireless links suffer from limited capacity, time-varying behavior, interference, etc. As a result, Bit Error Rate (BER) of the wireless medium (10^{-3} – 10^{-1}) is several

---

[1] This work is supported by Italian ministry in the framework of WORLD (Wireless multiplatfOrm mimo active access netwoRks for QoS-demanding muLtimedia Delivery) project.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 68–77, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

magnitudes higher than that of the wired links ($10^{-8} – 10^{-6}$) [3]. TCP interprets each loss as congestion-related and reacts by reducing its sending rate to a half of its size. The phase of congestion window increase is linear and takes considerable amount of time to compensate even a single such reduction of the sending rate.

The problems of TCP performance over wireless links are well-known [4]. The Forward Error Correction (FEC) technique applied to the TCP stream is one of the main solutions compensating the main problem, i.e. high error rate. FEC can be applied locally at the wireless link [4, 5] or at the end-to-end basis [6].

The FEC technique reduces packet loss probability at the expense of the bandwidth available for data transmission. While static FEC strength is commonly tuned to the worst error rate evidenced at the wireless link, dynamic control of the FEC strength, i.e. the amount of added redundancy, is required to maintain a reasonable TCP performance over heterogeneous networking scenarios.

Adding dynamic redundancy as a function of network state is proposed in [7-10]. Such schemes try to keep the amount of the redundancy added at the sender in accordance with error rate level estimated at the receiver side. As a result, the performance of dynamic FEC schemes depends on three components: wireless link error rate and accuracy of its estimation, end-to-end delay as measurements should be fed back from the receiver to the sender node, and bandwidth of the connection. These measurements are often inaccurate.

The design of forward error correction for TCP is shown to be dependent on the underlying random packet loss and distribution process. In [11], Loss-Tolerant TCP (LT-TCP) is proposed for extreme environments. It estimates the distribution of link errors and tunes its hybrid ARQ/FEC component accordingly. The authors of [12] propose a dynamic FEC assisted with cross-layer interaction from the link layer reporting the type of loss occurred. The approach proposed in [13] adapts channel estimation for the vehicular speeds, while the authors of [14] improve channel estimation by enabling Explicit Loss Notification (ELN) from network routers.

Summarizing, current proposals for dynamic FEC try to follow highly dynamic wireless channel state and, thus, struggle with inaccuracy of channel, end-to-end delay, and capacity estimation.

In this paper, we propose an FEC technique which adaptation is not a function of a network (or link) state, but a function of TCP mechanics. The proposed technique, called TCP-aware FEC, can be either end-to-end if implemented at the TCP sender or a local solution if it operates at the wireless link only.

The main design principle of TCP-aware FEC is that the amount of added redundancy is defined as a function of TCP window (or sending rate). This ensures tighter integration of FEC technology into TCP congestion control and helps to further improve the performance by increasing redundancy and protecting from error propagation into data segments with higher impact on TCP flow performance.

The rest of the paper is organized as follows: Section II provides the background on FEC and TCP flow and congestion controls, presents the core of the proposed approach and discusses its possible operation scenarios; Section III aims at presenting details of the simulation scenario and discussing the obtained results; Section IV concludes the paper outlining several points for the discussion and defining directions for future work on the topic.

2 TCP-Aware Forward Error Correction

Before presenting the core functionality of the proposed approach, it is important to understand the details of TCP congestion control algorithm and basic FEC operation.

2.1 Forward Error Correction

Forward Error Correction (FEC) is a technique allowing the data sender to add redundant data to the messages in order to help the receiver to detect and correct a limited number of errors in the received data flow without requesting for retransmission. At the packet level, FEC encoder operates with block codes, adding R redundancy packets to the block of K data packet and sending resulting N=R+K packets. One of the most widely used block error correction codes in wireless systems is Reed-Solomon code [16]. It allows correction of errors until their number does not exceed a half of the added redundancy code. This defines the tradeoff between the portion of bandwidth used for data transmission and the level of error protection offered.

For TCP, it is always desirable leaving the most of the bandwidth for data transmission until this level of bandwidth can be reached by TCP window evolution algorithm (under a given error rate on the channel). The dependence between TCP sending rate and channel errors are defined by the square root formula in [15].

However, it appears that the impact of transmission errors is not uniform and it depends on the position of erroneous packets within the TCP flow.

2.2 TCP Flow and Congestion Control

The most widely diffused version of TCP protocol in the Internet is TCP NewReno [17]. It employs Additive Increase Multiplicative Decrease (AIMD) as congestion window evolution strategy. TCP connection is initiated with congestion window (W) equal to one packet and Slow Start Threshold (*ssthresh*) set to a maximum possible value. Then, W is increased by one for every received non-duplicate ACK, until the *ssthresh* is reached. This represents the slow start phase and its basic idea is to provide a fast (roughly exponential over time) window increase till the capacity of the transmission pipe is reached.

Once the capacity is reached and the packet loss is detected by three consecutive duplicate ACKs, W is halved and TCP enters congestion avoidance phase. In this phase, the TCP sender gently probes the network for available bandwidth with a linear increasing window by $1/W$ for every TCP ACK received.

2.3 TCP-Aware FEC

Fig. 1 illustrates AIMD window evolution strategy and the proposed FEC strength protection. Stronger FEC is added for low TCP window values (W_{min}), which happen after congestion-related drop occurred, while weaker FEC is employed as the window approaches W_{max} (which corresponds to the congestion window value before the last packet loss).

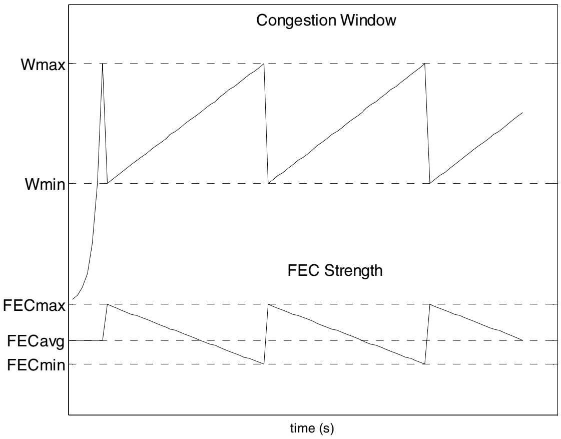


Fig. 1. TCP-aware FEC strength evolution

Any link-related packet loss will trigger unnecessary window reduction. However, for small window values, it will further decrease the throughput getting the flow away from available capacity. The actual value of the available end-to-end bandwidth is located between W_{min} and W_{max}. As a result, when current window value is close to W_{min}, the number of link errors should be minimized by adding stronger FEC – allowing the flow to increase throughput faster.

On the other hand, when congestion window is close to W_{max}, TCP sending rate is higher than end-to-end link capacity. The exceeding portion starts filling up the buffers and the probability of experiencing congestion loss increases. In this situation, the level of FEC protection can be reduced, since a congestion loss (and not a link error) will be likely to occur.

Based on such reasoning, the proposed FEC linearly varies the amount of added redundancy between FEC_{max} and FEC_{min} values, i.e. reversely proportional to the TCP window evolution. The linear function is chosen to be in line with AIMD window evolution strategy. However, for other TCP implementations like BIC TCP [18] or Compound TCP (CTCP) [19], it could be adapted accordingly.

2.4 Implementation and Deployment Scenarios

Fig. 2 presents two possible scenarios for TCP-aware FEC implementation: end-to-end and local.

End-to-end TCP-aware FEC is implemented either as a part of transport layer or directly below it, both at the TCP sender and the receiver side. This is the most suitable scenario for TCP-aware FEC implementation. The FEC coder can easily obtain information about current value of the congestion window and have instant signaling notification in case of congestion-related loss is occurred from TCP layer.

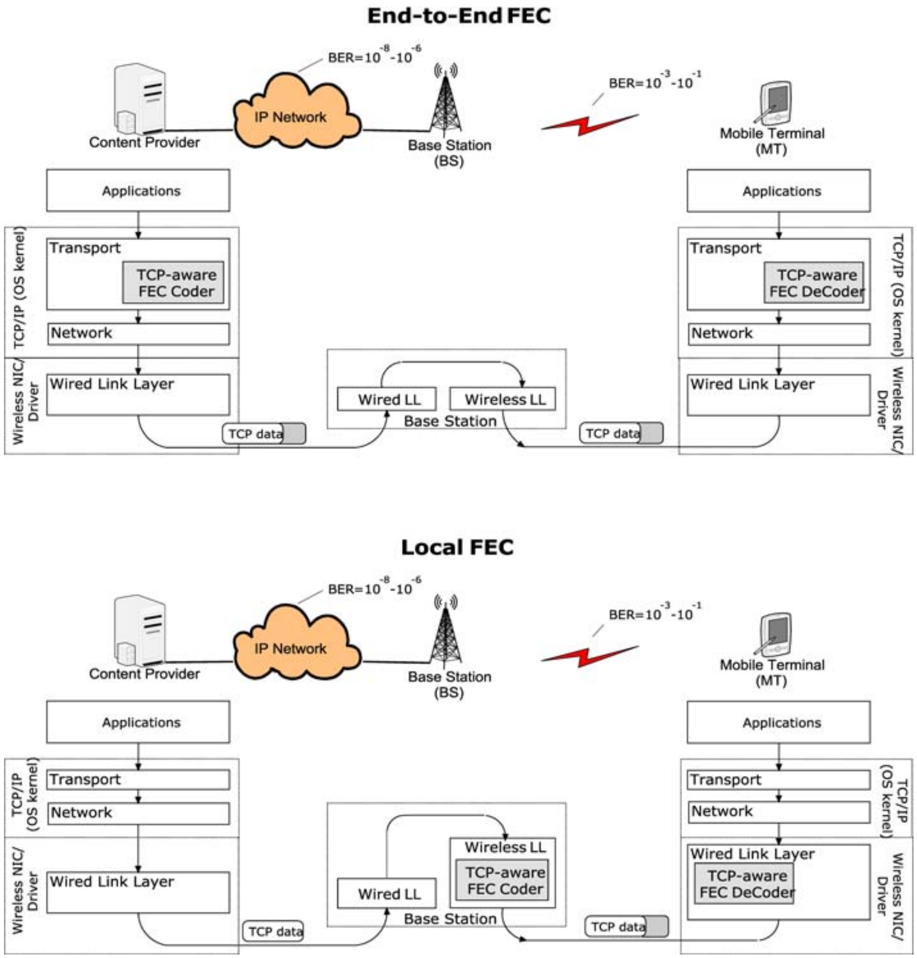


Fig. 2. TCP-aware FEC implementation scenarios

In this scenario, once the redundancy is added to the packet, it propagates to the receiver end without any modification – traversing fixed and wireless parts of the connection. At a first sight, this could be considered as a disadvantage, since no FEC protection is needed for the wired network (where error rate is low and added redundancy consumes unnecessary bandwidth). However, it appears that in most scenarios, the wireless last mile link represents the bottleneck of the end-to-end connection, while the bandwidth of the wired part remains underutilized. In fact, most of the proposals for coupling FEC and TCP operate in such end-to-end scenario.

Local TCP-aware FEC is implemented at the link layer and covers the wireless part of the end-to-end connection only. From the deployment point of view, this solution is more flexible, as it can be implemented within the wireless equipment (inside wireless cards or an OS driver) and be deployed and used where/when needed. In contrast, end-to-end implementation would require insertion of TCP-aware FEC module into the part of the protocol stack (TCP and IP layers) implemented inside OS kernel.

A drawback of local implementation lies in the requirement for the base station to track TCP flow related parameters, such as current congestion window, which is not always trivial and may require availability of additional computational and storage resources at the base station.

Taking into account the above mentioned disadvantages, the end-to-end scenario is chosen as preferred for TCP-aware FEC implementation over the "local" scenario. Nevertheless, local implementation is also possible in several operating scenarios.

3 Performance Evaluation

In order to perform performance evaluation of the proposed approach, we extended the Network Simulator (ns-2) [20] with the required functionalities. TCP-aware FEC was implemented at the end-to-end basis and redundancy information was added to every TCP packet leaving the source node.

TCP NewReno [17] is selected to operate at the transport layer, and its goodput (i.e. the amount of data successfully delivered to the destination) is chosen as the main performance metric.

3.1 Simulation Scenario

Fig. 3 presents the details of the simulation scenario. It is composed of two content provider nodes CP_1 and CP_2, one router R_1, two base stations BS_1 and BS_2, and two mobile terminal nodes MT_1 and MT_2. The network nodes located in the wired part of the network are interconnected with 10 Mb/s, 2 ms links. The wireless links are configured according to the IEEE 802.11b standard, with the configuration parameters reported in Table 1. Buffers at the base stations BS_1 and BS_2 are limited in size to 500 packets.

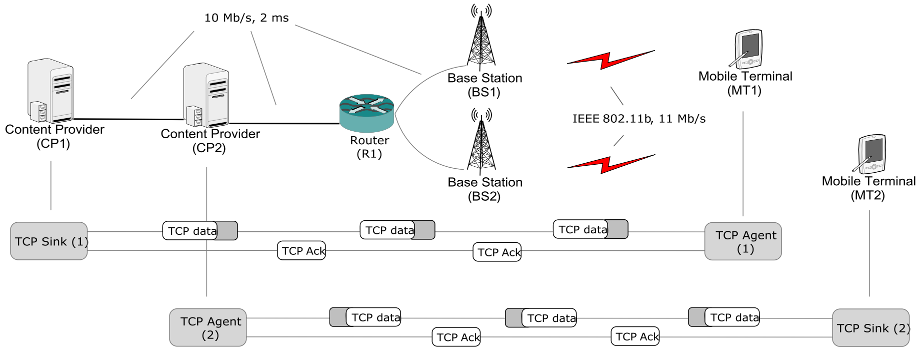


Fig. 3. Simulation scenario

Table 1. Simulation Parameters

Parameter Name	Value
Slot	20 μs
SIFS	10 μs
DIFS	50 μs
PLCP preamble + header	192 μs
Data Rate	11 Mbps
Basic Data Rate	1 Mbps
Propagation Model	two-ray ground

The wireless link error model follows uniform distribution, with BER in the range of 10^{-5} to 10^{-1}. FEC strength is expressed as the number of bits that can be corrected per packet (which was in range between 0 and 6 bits).

The duration of each simulation is 250 seconds, and the results reported are averaged from 10 runs with 95% confidence interval.

Two configurations for TCP flow are considered: one originated at CP_1 and a destination MT_1, another between MT_2 and CP_2. Only one flow is active at any time during the simulation. The main idea behind having flows in two different directions is to test the proposed approach for different locations of bottleneck wireless link. In the first case, it is located at the end of the connection (last mile); while in the second case it is the link connecting TCP sender (first mile).

The results obtained for both flows are essentially similar and in line with the expectation. For that reason, only those obtained for the connection between CP_1 and MT_1 are reported.

3.2 Results

Fig. 4 presents the results of a TCP connection throughput for different FEC strengths (from 0 to 6 bits), when the correction is applied constantly (and the amount of added redundancy is stable for the duration of the experiment) as well as for the dynamic TCP-aware FEC.

For low error rates (BERs smaller than 10^{-5}), all the schemes behave equally well with a minor difference in TCP throughput accounting for the overhead of added redundancy. However, when BER becomes higher than 10^{-5}, the flows with low FEC strength start to rapidly decrease their throughput. As expected, the flow with the strongest FEC of 6 bits remains insensitive to errors longer than other flows.

The curve corresponding to the TCP-aware FEC lies in the middle. It outperforms fixed FEC solutions when FEC strength is low (less than 4 bits). However, falls short when the error rate becomes large.

The main advantage of using TCP-aware FEC is in its capability to preserve excessive usage of bandwidth for transmitting redundancy information. In TCP-aware FEC, the amount of added redundancy is the function of congestion window and thus it depends on the BER of the wireless channels.

Fig. 5 presents the amount of total redundancy added during the simulation time as percentage of the actual data flow for a wireless channel with BER equal to 10^{-3}. It can be seen that TCP-aware FEC outperforms approaches with fixed FEC strength for all the evaluated values.

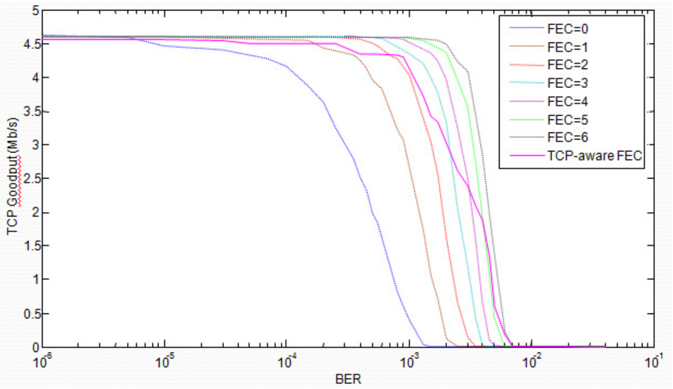


Fig. 4. TCP goodput performance for different FEC schemes in erroneous channels

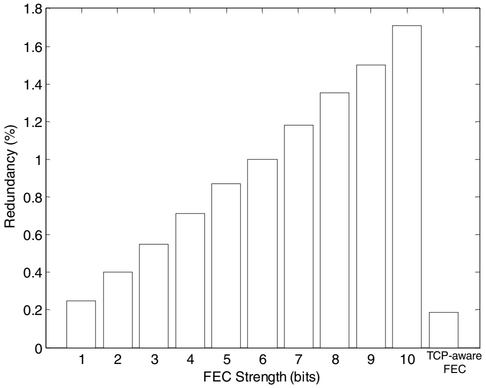


Fig. 5. Comparison of total redundancy added by different approaches

4 Conclusions and Future Works

This paper presents a novel approach for error correction TCP-aware FEC. The amount of redundancy added at the sender node to TCP packets is computed as a function of TCP window size. TCP-aware FEC becomes stronger for low window values experienced after a packet loss is detected and the window is reduced to its half, while for large congestion windows approaching end-to-end capacities the amount of added redundancy is reduced.

Driven by the TCP congestion and flow control mechanics, the proposed solution varies the level of error protection protecting TCP from incorrect (due to link losses) decisions for window reductions.

The proposed FEC scheme can be implemented either end-to-end as a part of TCP sender and receiver protocol stacks, or locally covering wireless part of the connection only.

Simulation results confirm an excellent tradeoff between the level of offered error protection and the amount of total redundancy added to the TCP flow for TCP-aware FEC.

Future directions for the approach will deal with implementation of the proposed technique as a patch for OS Linux kernel and extensive wide-area network experiments.

References

1. Fraleigh, C., Moon, S., Lyles, B., Cotton, C., Khan, M., Moll, D., Rockell, R., Seely, T., Diot, S.C.: Packet-level traffic measurements from the Sprint IP backbone. IEEE Network 17(6), 6–16 (2003)
2. Bakin, D.S., Joa-Ng, M., McAuley, A.J.: Quantifying TCP Performance Improvements in Noisy Environments Using Rotocol Boosters. In: Fifth IEEE Symposium on Computers and Communications (2000)
3. Pentikousis, K.: TCP in wired-cum-wireless environments. IEEE Communications Surveys 3, 2–14 (2000)
4. Balakrishnan, H., Padmanabhan, V.N., Seshan, S., Katz, R.H.: A comparison of mechanisms for improving TCP performance over wireless links. IEEE/ACM Transactions on Networking (TON) 5(6), 756–769 (1997)
5. Barakat, C., Altman, E.: Bandwidth tradeoff between TCP and link-level FEC. Computer Networks 39(2), 133–150 (2002)
6. Lundqvist, H., Karlsson, G.: TCP with end-to-end FEC. In: International Zurich Seminar on Communications, pp. 152–155 (2004)
7. Baldantoni, L., Lundqvist, H., Karlsson, G.: Adaptive end-to-end FEC for improving TCP performance over wireless links. In: IEEE International Conference on Communications, vol. 7, pp. 20–24 (June 2004)
8. Park, K., Wang, W.: AFEC: an adaptive forward error correction protocol for end-to-end transport of real-time traffic. In: International Conference on Computer Communications and Networks (1998)
9. Tsugawa, T., Fujita, N., Hama, T., Shimonishi, H., Murase, T.: TCP-AFEC: An adaptive FEC code control for end-to-end bandwidth guarantee. Packet Video, 294–301 (November 2007)
10. Liu, B., Goeckel, D.L., Towsley, D.: TCP-cognizant adaptive forward error correction in wireless networks. In: IEEE Global Telecommunications Conference (GLOBECOM), vol. 3, pp. 2128–2132 (November 2002)
11. Subramanian, V., Kalyanaraman, S., Ramakrishnan, K.K.: An End-to-End Transport Protocol for Extreme Wireless Network Environments. In: Military Communications Conference, MILCOM (2006)
12. Baroudi, U., Abu Qadous, B.: An efficient adaptive Cross-Layer interaction mechanism for TCP traffic over heterogeneous networks. In: IEEE Symposium on Computers and Communications, pp. 118–123 (2008)
13. Ahmad, I., Habibi, D., Rahman, Z.: An Improved FEC Scheme for Mobile Wireless Communication at Vehicular Speeds. In: Telecommunication Networks and Applications Conference, pp. 312–316 (December 2008)
14. Miyoshi, M., Sugano, M., Murata, M.: Performance improvement of TCP on wireless cellular networks by adaptive FEC combined with explicit loss notification. IEEE Vehicular Technology Conference (VTC Spring) 2, 982–986 (2002)

15. Mathis, M., Semke, J., Mahdavi, J., Ott, T.: The macroscopic behavior of the TCP congestion avoidance algorithm. ACM SIGCOMM Computer Communication Review 27(3), 67–82 (1997)
16. Immink, K.A.S.: Reed–Solomon Codes and the Compact Disc. In: Wicker, S.B., Bhargava, V.K. (eds.) Reed–Solomon Codes and Their Applications. IEEE Press, Los Alamitos (1994)
17. Floyd, S., Henderson, T.: The NewReno Modification to TCP's Fast Recovery Algorithm. Request for Comments 2582, ETFC (April 1999)
18. Xu, L., Harfoush, K., Rhee, I.: Binary increase congestion control (BIC) for fast long-distance networks. INFOCOM 4, 2514–2524 (2004)
19. Tan, K., Song, J., Zhang, Q., Sridharan, M.: A compound TCP approach for high-speed and long distance networks. Microsoft Press, MSR-TR-2005-86 (July 2005)
20. The network simulator ns2, `http://www.isi.edu/nsnam/ns`

Delay Performance Analysis of a Two-Stage Cross-Layer Scheduler for Wireless LANs

Andreas Könsgen and Carmelita Görg

Center for Computing Technologies (TZI)
University of Bremen
Otto-Hahn-Allee 1, 28359 Bremen, Germany
{ajk,cg}@comnets.uni-bremen.de

Abstract. The transport of real-time data flows over wireless channels can be optimized by cross-layer schedulers which serve the different users dependent on their traffic load and channel state. This paper investigates the delay performance of a two-stage cross-layer scheduler which has been designed to meet the above requirements. The well-known Weighted Fair Queuing Scheduler can tramsmit packets within a guaranteed delay that can be analytically determined, however the delay cannot be adjusted directly. The latter is possible with the scheduler discussed in this paper, where a transmission is performed in a stochastic way which means a certain percentage of the packet is lost, which is however often tolerable for applications such as video or VoIP. An analytical approach of the delay performance of the scheduler is given and validated by simulation results.

Keywords: Cross-Layer, Scheduling, Wireless LAN, Quality-of-Service.

1 Introduction

The transport of data streams for real-time applications over wireless networks includes challenges. The radio channel is usually time-variant so that prerequisites have to be taken in order to maintain troughput and delay constraints required by the application. A widely used scheduling mechanism for communication networks in general is the Weighted Fair Queueing Scheduler. The "original" version of that scheduler however assumes a transmission media with constant physical bit rate. Given a number of data flows belonging to different users and assuming that the sum of all traffic loads does not exceed the capacity of the line, it guarantees the delivery of each packet within a delay that is dependent on the weights assigned to the different flows. By means of the weighting factors, the scheduler considers the different traffic loads of the flows so that each of them gets a portion of the channel capacity proportional to its traffic load. This however means that there is no direct way to adjust the delay of the packets immediately; the delay can be expressed analytically, it is however a dependent variable of the weighting factors which are dependent on the throughput. The same is true for extensions of the WFQ scheduler for wireless networks, as they for example have been proposed in [1]. In the latter work, the WFQ scheduler

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 78–87, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

is extended to cope with varying channel capacities by monitoring if flows are leading or lagging. Similar to the unmodified WFQ scheduler, the article also gives an upper limit for the delay which is again dependent on the weighting factors. However, for the WFQ scheduler and its derivatives, the user can control the throughput for each flow by specifying a weighting factor. Regarding the upper boundary of the delay, a closed expression can be given which is dependent on the weighting factors. That means that the delay is constrained, but it is dependent on the throughput settings.

In this paper, a cross-layer scheduler is analyzed which has been introduced in previous publications such as [4]. In contrast to the WFQ scheduler, the scheduler discussed here allows the immediate setting of the throughput and the delay for time-critical flows, which has been investigated by simulations. In this work, an analytical model of the scheduler is developed which allows to determine if packets can be transmitted within a given time and if this behavior is deterministic – i. e. all packets can be transmitted – or stochastic, which means that there is a certain probability that a packet cannot be scheduled within the given delay constraint and hence has to be discarded. The latter, however, is tolerable for many real-time applications. In a video transmission, a missing frame is hardly noticed by the viewer; in case of VoIP, some missing audio samples do not severely affect the quality of the phone call. The task of this paper is to give a quantitative analysis of the delay characteristics and the packet loss probability dependent on the channel load.

2 Structure of the Scheduler

Investigations on cross-layer scheduling are an important research topic in recent years. For example, the scheduling concept presented in [2,3], which is specially designed for OFDM-TDMA transmissions and integrates the channel state into the MAC layer scheduling. In the approach presented in this paper, TDMA is used as well, however the PHY scheduling is separated from the MAC scheduling; the schedulers communicate through an abstract interface, i. e. providing an importance metric instead of giving detailed information about packet lifetime etc. Two scheduling concepts are analyzed in [6], where one has a better support for QoS and the other one has a better support for the total throughput. The investigations presented here focus on the delay, which is important from the view of the user, whereas a provider aims to maximize the total throughput. Fair scheduling in wireless networks is, besides the previously mentioned work [1], widely investigated, for example in [7] or [8], whereas the latter work also differentiates between different QoS classes.

The design of the cross-layer scheduler discussed in this paper is given in fig. 1. The scheduler includes two stages: in the MAC layer stage, a queue is maintained for each data flow. In each turn of the scheduler, one or more packets are selected and handed over to the physical layer scheduler, along with a priority value which is determined according to the MAC scheduling scheme, which has knowledge about the QoS requirements throughput and delay of the data flows,

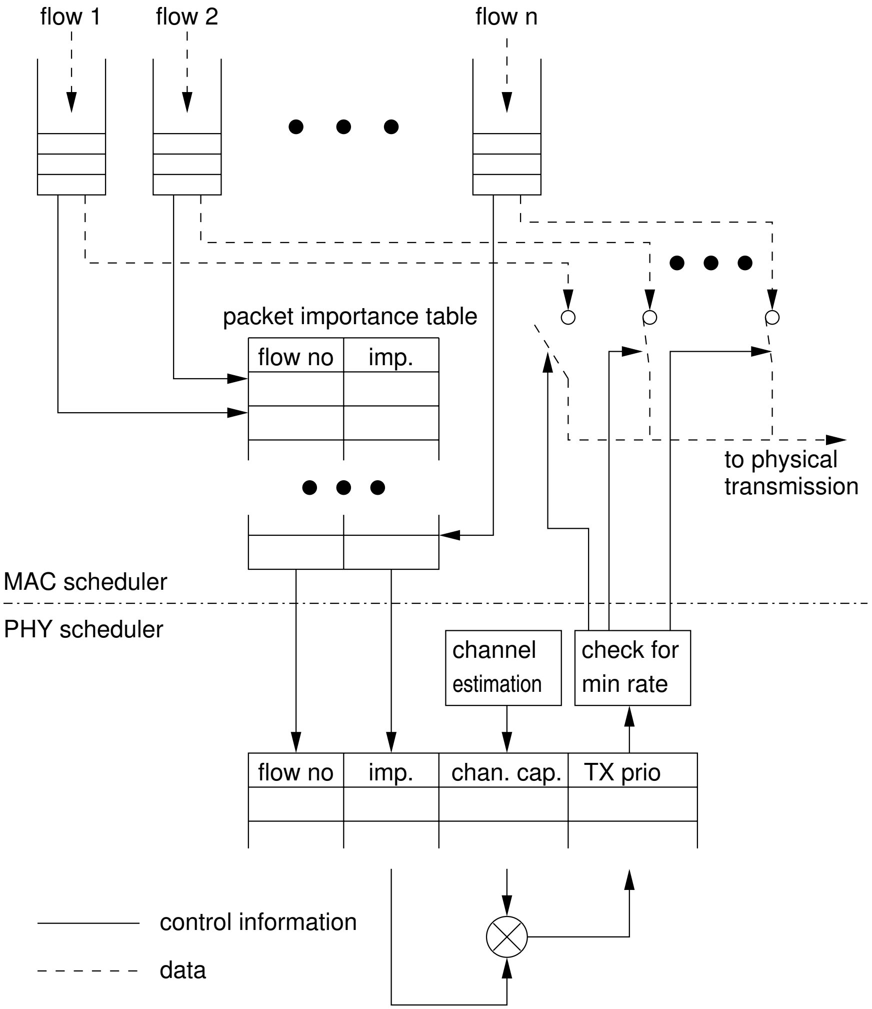


Fig. 1. Design of the cross-layer scheduler

also it keeps track about the packets which have been successfully transmitted in the past and about the packet lifetime. While the throughput is determined by a sliding window which monitors the packets transmitted within a particular time span, the delay control is maintained by assuming that the packets have a limited lifetime until they are transmitted. While the packet is waiting for transmission, the remaining lifetime is counted down; if it reaches zero, the packet is discarded. In order to calculate the final priority out of the throughput and delay measurements, the latter is converted by a weighting function; after that the results both for the throughput and the delay are added to determine the priority. After this operation has been completed for each data flow which has a packet ready to be sent, the selected packets are handed over to the physical layer part of the scheduler along with their priorities. The PHY layer scheduler supports different transmission schemes – TDMA, OFDMA, SDMA – which can be selected by the user. Dependent on the active scheme and the channel conditions, one or more packets which have been handed over by the MAC layer scheduler are selected for transmission. The MAC layer scheduler gets a feedback which packets were actually sent so that it can update the state of its queues.

For the investigations, only the downlink is considered. In this paper, the above scheduler model which has been used in previous investigations is simplified to allow an analytic description of the delay performance: the priority is calculated only based on the measurements of the remaining lifetime.

3 Analytical Modeling

Analytical considerations regarding the throughput performance of the above-mentioned scheduler have been given in [5]. In this paper, the delay characteristics of the scheduler described above are investigated. n data flows are considered, where each of them is maintained by its own queue. It is however assumed that the load generator generates a packet whenever the previous one has been successfully transmitted, so that the queue length is 1 and each station always has a packet to transmit. TDMA is used as the transmission method so that exactly

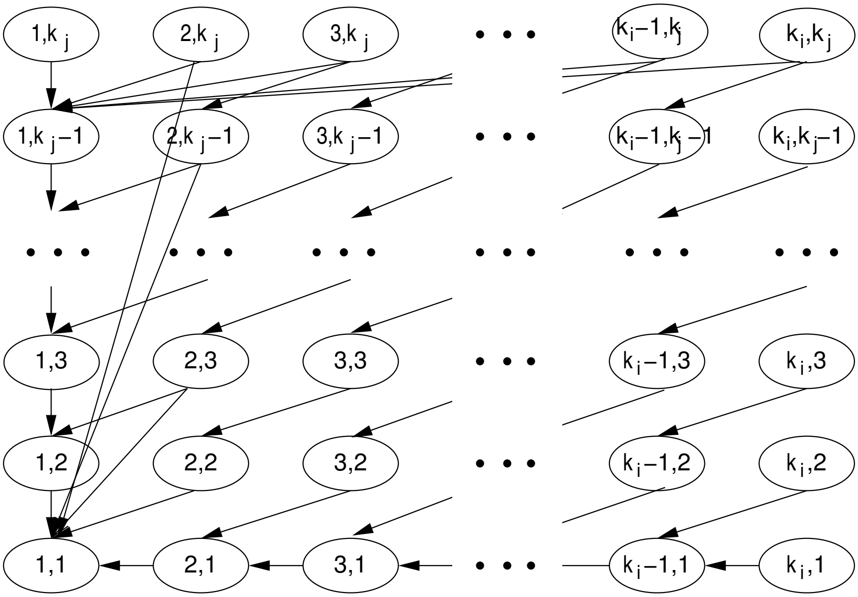


Fig. 2. Transition diagram for two data flows. The oval symbols identify the states of the system, the numbers identify the remaining lifetime for flows i and j.

one flow is served at each time. Constant packet size is assumed, the channel is time-variant in such a way that the transmission time of a packet is uniformly distributed with the mean value T, the minimum $T_{\min}$ and the maximum $T_{\max}$. It is assumed that $T_{\min}$ and $T_{\max}$ are the same for all flows. The throughput control of the above scheduler is not considered for the analytical investigations, because it affects the priority of individual packet dependent on events in the past. Since the presented approach is based on a Markov chain, it is however required that the next state of the system only depends on the current one.

Considering the fact that exactly one packet of one flow is served at a time, this means that in average the other flows have to wait for the time interval T until the scheduler serves the next packet. For simplicity, it is assumed that the maximum age of a packet is an integer multiple of the slot length T; the maximum age of a packet belonging to flow i can then be expressed as the maximum number of time slots $k_{\max,i}$ the packet may wait in the queue until it expires.

With these prerequisites, the scheduling policy can be modeled by an n-dimensional Markov chain, where each dimension represents the number of time slots that the packet of a particular flow has left until it expires. Each state in the chain is identified by an n-tuple giving the number of time slots k_i which are remaining for the next packet of flow i until expiration, i. e. $(k_1, k_2, \ldots, k_n)$. If flow i is served and thus the next packet is provided by the load generator, then k_i is set to the lifetime of the new packet $k_{i,\max}$, whereas for the other flows $j \neq i$ the respective k_j are decremented by 1. If the packet of flow i expires before transmission, the next packet is provided and k_i is reset as in the case of a successful transmission. Fig. 2 shows the state diagram for two flows i, j. In a system of n flows, the diagram shows two dimensions out of an n-dimensional cube. For reasons of overview, the tuples which identify the states only give the indices for the two dimensions i, j shown in the diagram.

If none of these two flows is served, the lifetime for both packets inside flow i and j is reduced by 1, so that the system moves from (k_i, k_j) to $(k_i - 1, k_j - 1)$, i.e. along the arrows running in a diagonal, pointing to the lower left. If flow i is served or the lifetime of flow i has expired, the system moves from (k_i, k_j) to $(k_{i,\max}, k_j - 1)$ which results in an arrow pointing horizontally to the rightmost column of the diagram. Likewise, a service of flow j means moving to $k_i, k_{j,\max}$ denoted by an arrow pointing vertically to the row at the bottom of the figure.

In order to determine the QoS characteristics of the scheduler, the probability must be known that a flow is served before its lifetime expires. It is assumed that each flow has a uniform distribution of the transmission time with the same $T_{\min}$ and $T_{\max}$ as specified above. In order to determine the transmission priority β_i of flow i, the transmission time T_i which the flow experiences at the current moment due to the channel conditions is divided by a weighting factor $w(k_i)$ which is dependent on the remaining lifetime of the packet k_i:

$$\beta_i = T_i / w(k_i). \tag{1}$$

The flow with the smallest priority value $\min_i \beta_i$ is served next. $w(k_i)$ must be a strictly monotonic increasing function; in this paper, the proportionality $w(k) = k$ is used.

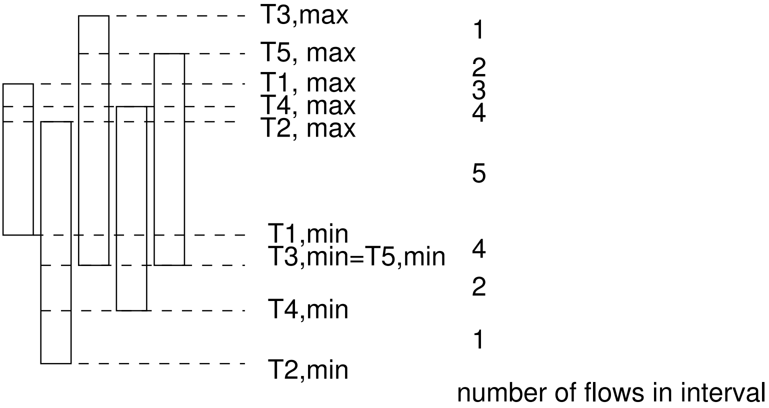


Fig. 3. Calculating the transition probability

The priority β is dependent on the randomly distributed transmission time T, hence the priority itself is a random variable. In order to determine the transition probability from one state to another one, for each of the n flows the probability that the respective flow is served in the next turn must be determined. For n flows with uniformly distributed transmission times and the same $T_{\min}$ and $T_{\max}$, where in each scheduling turn the flow with the smallest transmission time T is selected, the service probability for any of the flows is $1/n$ because of symmetry reasons. As already mentioned, the transmission times are mapped to priorities by weighting factors which are dependent on the packet age of the respective flow. If flow i has a remaining lifetime of k_i, its priority values range between $\beta_{i,\min} = T_{\min}/k_i$ and $\beta_{i,\max} = T_{\max}/k_i$ dependent on the channel condition. The different flows usually experience different weighting factors so that the resulting intervals $[\beta_{i,\min}, \beta_{i,\max}]$ might or might not be overlapping. In order to calculate the service probability for a particular flow, the $\beta_{\min}$ and $\beta_{\max}$ of all n flows are sorted in a common list in ascending order: $\beta'_1 \le \beta'_2 \le \ldots \le \beta_{2n}$. Out of this list, intervals $[\beta'_1, \beta'_2]$, $[\beta'_2, \beta'_3]$, $\ldots$, $[\beta'_{2n-1}, \beta'_{2n}]$ are formed, which is illustrated in fig. 3. For each interval mentioned above, there is a certain probability q_i that a random sample β_i of a particular flow i is inside the interval. q_i is greater than zero if the following condition is met:

$$\beta_{\min,i} \le \beta'_j \quad \text{and} \quad \beta'_{j+1} \le \beta_{\max,i} \tag{2}$$

and can be calculated in this case as

$$q_i = \frac{\beta'_{j+1} - \beta'_j}{\beta_{\max,i} - \beta_{\min,i}}. \tag{3}$$

In a particular scheduling turn, for each flow i a random sample of β_i is drawn. Due to the probabilities q_i, in case of n flows, there are 2^n combinations for which flows the current random sample is inside the interval $[\beta'_j, \beta'_{j+1}]$. The flow indices i are mapped to values i' in a way that those l flows with random samples inside the interval are changed to $1 \leq i' \leq l$ and the other $n-l$ flows to $l+1 \leq i' \leq n$. Considering that for a given combination of l flows whose β is distributed inside the same interval for each flow, the probability that a particular flow is served is $1/l$ as mentioned earlier.

The probability has to be further conditioned due to the fact that only combinations within intervals which fulfil the inequality

$$\beta'_{j+1} \leq \min_i \beta_{\max,i} \tag{4}$$

contribute to the service of a flow. Expressed in words this means that combinations located in intervals not covered by above condition do not provide any service. For those latter intervals, there is always at least one flow which never occurs inside the interval because it has shorter transmission times and thus a smaller β. The probability that service is provided to flow l with $\beta_l \in [\beta'_j, \beta'_{j+1}]$ is then

$$p([\beta'_j, \beta'_{j+1}], l) = \frac{1}{l} \prod_{\alpha=1}^{l} q_\alpha \cdot \prod_{\alpha=l+1}^{n} (1 - q_\alpha) \quad \text{if eqn. (4) is met, 0 else.} \tag{5}$$

To determine the transit probability for one particular flow, all $p([\beta'_j, \beta'_{j+1}], l)$ for this flow have to be summed up for all possible combinations.

If the current system state is $(k_1, \ldots, k_i, \ldots, k_n)$ and flow i is served, the next state is then $(k_1, \ldots, k_{i,\max}, \ldots, k_n)$. When defining $M = \{\text{flow1}, \ldots, \text{flow}l\}$, the transition probability $p_{\mathrm{tr},i}$ for this flow is then:

$$p_{\mathrm{tr},i} = \sum_{\text{all } [\beta'_j, \beta'_{j+1}], M} \; \sum_{\text{all combinations}} p([\beta'_j, \beta'_{j+1}], l). \tag{6}$$

After calculating the transition probabilities, the stationary probabilities of the states have to be determined. In order to do so, first the Markov chain with m dimensions with the lengths $k_{1,\max}, k_{2,\max}, \ldots, k_{m,\max}$ is mapped to a one-dimensional one with the length $A = \prod_{i=1}^{m} k_i$ by transforming the tuple $(k_1, \ldots k_m)$ of a state to a scalar index with the range 1 . . . A. Out of this chain, a squared transition matrix with the size $A \times A$ can be written which has the form

$$\begin{pmatrix} p(1|1) & \ldots & p(1|A) \\ \ldots & \ldots & \ldots \\ p(A|1) & \ldots & p(A|A) \end{pmatrix}. \tag{7}$$

This matrix must fulfil the condition that the sum of the matrix coefficients in each row must be one. With the further condition that the sum of all stationary probabilities must be 1, a linear equation system can be formed which can be solved by numerical means.

An important QoS metric is the loss probability due to expiry of the packet lifetime. With the known stationary probabilities, the loss probability is the probability of transiting from state 1 back to state n, which is $p(1) \cdot p(n|1)$.

By means of the Markov chain, it can be determined what are the requirements that all packets can be transported and what is the delay in this case, as well as it can be determined under which conditions packet loss occurs and what is the amount of this packet loss. The probability that a packet for flow i is transmitted after exactly r trials can be determined by summing up the stationary probability for all states which include $k_i = k_{i,\max} - r$. In this way, the discrete distribution function for each flow can be easily calculated.

The probability for a packet loss of flow i is the sum of the transition probabilities for all states with $(k_1, \ldots, k_i = 1, \ldots, k_n)$ to the respective corresponding state $(k_1, \ldots, k_i = k_{i,\max}, \ldots, k_n)$.

4 Comparison between Analytical and Simulated Results

In the simulation setup, the CCDF for the waiting time which each of a number of flows experiences is determined. 4 flows are considered, where one has a delay

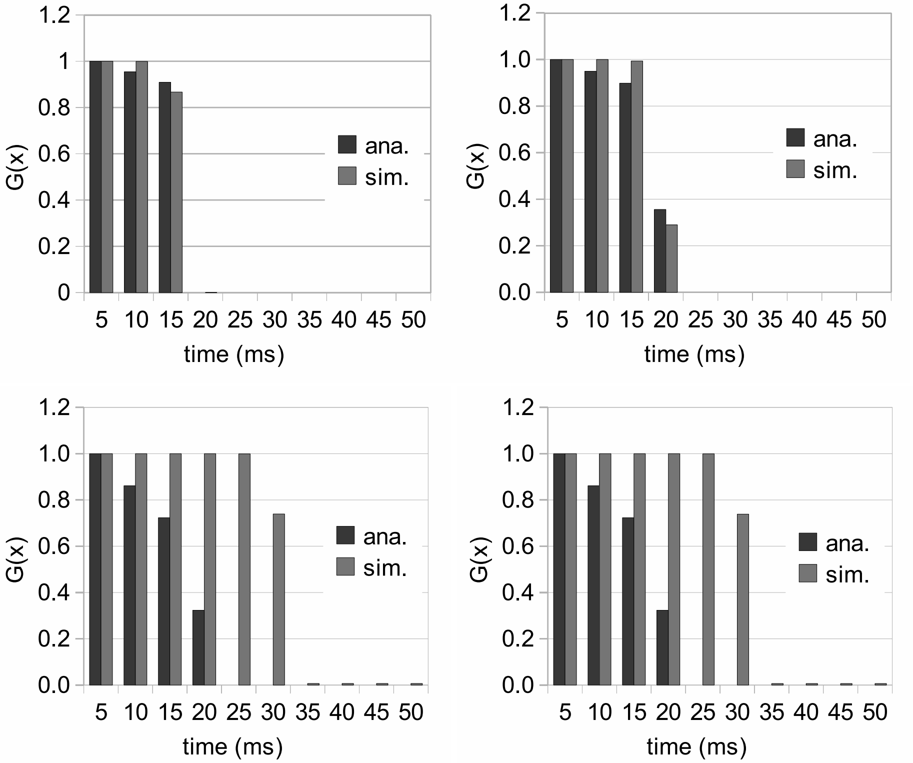


Fig. 4. CCDF of the waiting time for the four flows

constraint of 20 ms, one has 30 ms and the other two have 40 ms. The transmission time varies between 4.5 and 6.5 ms which means with a mean value of 5 ms. Fig. 4 shows the distribution function for the waiting time for each of the four flows. Precisely, the value which is counted to generate the figure is number of scheduling cycles which elapse until the next packet for a particular flow has been served. Assuming the mean value of 5 ms for a packet transmission, the number of scheduling cycles can however be interpreted as the transmission time. The simulation results for the delay and the packet loss rate are compared with the results from the theoretical analysis.

It can be seen that the scheduling scheme keeps the constraints for the respective delays between 20 and 40 ms. Only a small amount of packets exceeds the limit and has to be discarded.

For the flows with a limit of 20 or 30 ms, the analytical results are well matched by the simulation. For the flows with 40 ms delay, the simulations yields higher delays than the analytical consideration. The reason is that the assumption of constant transmission time for each packet which was needed for the theoretical analysis is an approximation. In the theoretical approach, the priorities which are calculated for the packets hence are discrete values. In the stochastic simulation, the priority values are continuous.

5 Conclusions

The scheduler discussed in this paper differs from the well-known WFQ scheduler in two ways: on the one hand, it is possible to specify a given maximum delay for the packets being delivered over the radio network. On the other hand, it cannot be guaranteed that all packets can be delivered within a given time, hence the scheduler behaves in a probabilistic way. In contrast to this, the WFQ scheduler is deterministic in the sense that it can deliver all packets within an upper boundary for the delay that can be analytically deduced, however it is not possible to specify a maximum delay that the scheduler has to meet; the delay is a result of the weighting factors which determine the throughput which the scheduler should allocate for each data flow, i.e. it does not allow to configure the delay independently from the throughput. For applications requiring bitwise precise transmissions, this means the WFQ is more suitable due to its deterministic behavior of transporting all packets. However, for real-time applications, the proposed scheduler can be more useful, since it can meet delay boundaries while the application in many cases tolerates packet loss by a certain amount. The probability of a packet loss is dependent on the total channel load, it increases the more data has to be transported.

References

1. Wang, Y.-C., Tseng, Y.-C., Chen, W.-T., Tsai, K.-C.: MR-FQ: A Fair Scheduling Algorithm for Wireless Networks with Variable Transmission Rate. Simulation 81(8) (2005)

2. Haleem, M.A., Chandramouli, R.: Adaptive Downlink Scheduling and Rate Selection: A Cross-Layer Design. IEEE Journal on Selected Areas in Communications 23(8) (2005)
3. Haleem, M.A., Chandramouli, R.: Adaptive Stochastic Iterative Rate Selection for Wireless Channels. IEEE Comm. Letters 8(5) (2004)
4. Könsgen, A., Timm-Giel, A., Görg, C., Böhnke, R.: Impact of the Transmission Scheme on the Performance of Wireless LANs. In: Proc. Mobilight, Athens, Greece (2009)
5. Könsgen, A., Islam, M., Timm-Giel, A., Görg, C.: Performance Analysis of Packet Aggregation in WLANs with Simultaneous User Access. In: Proc. IFIP, Aachen, Germany (2009)
6. Chen, B., Fitzek, F., Gross, J., Grünheid, R., Rohling, H., Wolisz, A.: Framework for Combined Optimization of DLC and Physical Layer in Mobile OFDM Systems. In: 6th Int. OFDM Workshop, Hamburg, Germany (2001)
7. Lu, S., Bhargavan, V., Srilant, R.: Fair Scheduling in Wireless Packet Networks. In: Proc. SIGCOMM (1997)
8. Song, J., Li, L., Han, J.: A Wireless Fair Scheduling Algorithm Supporting CoS. In: Proc. IEEE Int. Conf. on Communications, Circuits and Systems (2002)

Access Network Selection in a Heterogeneous Environment Using the AHP and Fuzzy TOPSIS Methods

Aggeliki Sgora[1], Periklis Chatzimisios[2], and Dimitrios D. Vergados[1]

[1] Department of Informatics
University of Piraeus
GR-185 34, Piraeus, Greece
`{asgora,vergados}@unipi.gr`
[2] Computing Systems, Security and Networks Research Lab
Department of Informatics
Alexander Technological Educational Institution of Thessaloniki
GR-57400, Sindos, Thessaloniki, Greece
`peris@it.teithe.gr`

Abstract. The problem of network selection across heterogeneous wireless networks has recently received much attention because of a drive for converged communication systems. However, since the selection of an access network depends on several parameters with different relative importance, such as the network and the application characteristics, the user preferences, the service cost, etc, it is a difficult task to be achieved. In this paper an effective access network selection algorithm for heterogeneous wireless networks is proposed that combines two Multi Attribute Decision Making (MADM) methods, the Analytic Hierarchy Process (AHP) method and the fuzzy Total Order Preference by Similarity to the Ideal Solution (TOPSIS) method. More specifically, the AHP method is used to determine weights of the criteria, and the fuzzy TOPSIS method is used to obtain the final access network ranking.

Keywords: Wireless Network; Network Selection; MADM; Heterogeneous Environment; AHP; TOPSIS; fuzzy TOPSIS.

1 Introduction

The increased need of users for ubiquitous service coverage and provision of different types of service leads to development of the heterogeneous networks. In such an environment, soon it will be very common for a user to hold a mobile device equipped with multiple interfaces in order to access all the wireless technologies of the heterogeneous network. However, since these wireless technologies differ widely in terms of their capabilities, cost and coverage, the selection of the optimal access network is a very challenging task.

The problem of network selection across heterogeneous wireless networks has recently received much attention because of a drive for converged communication systems. In this context, authors in [1] proposed the combined application of two mathematical

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 88–98, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

techniques in an algorithm for network selection between Universal Mobile Telecommunications System (UMTS) and wireless local area networks (WLANs). Work in [2] proposed network selection based on a resource allocation strategy for efficient resource utilization in a heterogeneous network environment. In [3], the authors evaluated heterogeneous networks, using measures of specific parameters from each network.

Moreover, since the selection of an access network depends on several parameters with different relative importance, such as the network and the application characteristics, the user preferences, the service cost, etc, the access network selection problem is usually looked at from the aspect of multi-criteria analysis, and more specifically by applying different Multi Attribute Decision Making (MADM) algorithms [4,5]. More specifically, Bari and Leung [4] apply the ELECTRE method in order to solve the problem of network selection. In [5] the authors propose the TOPSIS in order to rank the candidate networks for service delivery to the terminal. Work in [6] presented an approach that combines two methods, the AHP (Analytical Hierarchy Process) and GRA (Grey Relational Analysis) in order to evaluate the total QoS. Wu *et al.* [7] applied the AHP method to determine weights of their QoS criteria for the network selection. Charilas *et al.* [8] combined Fuzzy AHP and ELECTRE in order to assign weight to the criteria and to rank the candidate networks.

In this paper, we propose an effective access network selection algorithm for heterogeneous wireless networks that combines two MADM methods, the AHP method and the fuzzy Total Order Preference by Similarity to the Ideal Solution (TOPSIS) method. More specifically, the AHP method is used to determine weights of the criteria, and the fuzzy TOPSIS method is used to obtain the final access network ranking. The novelty of this approach is that instead of applying fuzziness during the determination of the weights, the fuzziness is applied during the ranking of the candidate networks. This comes from the observation that is much easier and more precise to determine the level of influence of the criteria than to characterize the value of a criterion, e.g. the security degree of a network. For this reason linguistic values are used for the evaluation of the candidate networks, and more specifically the fuzzy TOPSIS method presented [9] is used for the final access network ranking.

The rest of the paper is organized as follows: Section 2 provides an overview of the fuzzy set theory and Section 3 presents the MADM methods, AHP and fuzzy TOPSIS that are employed in our access network selection algorithm. Section 4 illustrates a numerical example of the proposed algorithm, whereas Section 5 concludes the paper and presents future research.

2 Fuzzy Set Theory Basics

2.1 Fuzzy Numbers

The Fuzzy set theory was first introduced by Zadeh [10] in order to deal with vague, imprecise and uncertain problems, and it has been used as a modeling tool for complex systems that can be controlled by humans but are hard to define precisely [11]. The theory is based on the fuzzy sets, i.e. sets, whose elements belong to the set with some degree of membership that is most commonly expressed by real numbers in the unit interval $[0,1]$.

Definition 1. Assuming that X is a set, then the fuzzy set $\tilde{A}$ on X is characterized by a membership function μ that associates with each element x in X a real number in the unit interval $[0,1]$.

Definition 2. A convex fuzzy variable $\tilde{\alpha}$ is referred as fuzzy number if its membership function $\mu_{\tilde{\alpha}}(x)$ is piecewise continuous and if has the functional value $\mu_{\tilde{\alpha}}(x) = 1$ at precisely one of the x values with $x = x_r = x_l = 1$ where

$$x_l = \min[x \in IR \mid \mu_{\tilde{\alpha}}(x) = 1] \text{ and } x_r = \max[x \in IR \mid \mu_{\tilde{\alpha}}(x) = 1]$$

In this paper triangular number is used in our model. A triangular fuzzy number is defined by a triplet $(\alpha_1, \alpha_2, \alpha_3)$. The membership function $\mu_{\tilde{\alpha}}$ of a fuzzy number $\tilde{\alpha}$ is given by

$$\mu_{\tilde{\alpha}}(x) = \begin{cases} 0 & x < a_1 \\ (x - \alpha_1)/(\alpha_2 - x) & a_1 \le x \le a_2 \\ (x - \alpha_3)/(\alpha_3 - \alpha_2) & a_2 \le x \le a_3 \\ 0 & x > a_3 \end{cases} \tag{1}$$

Assuming that $\tilde{A} = (\alpha_1, \alpha_2, \alpha_3)$, $\tilde{B} = (b_1, b_2, b_3)$ are two positive triangular fuzzy numbers, then the following operational laws can be defined:

$$\tilde{A}(+)\tilde{B} = (\alpha_1, \alpha_2, \alpha_3)(+)(b_1, b_2, b_3) = (\alpha_1 + b_1, \alpha_2 + b_2, \alpha_3 + b_3) \tag{2}$$

$$\tilde{A}(-)\tilde{B} = (\alpha_1, \alpha_2, \alpha_3)(-)(b_1, b_2, b_3) = (\alpha_1 - b_1, \alpha_2 - b_2, \alpha_3 - b_3) \tag{3}$$

$$\tilde{A}(\cdot)\tilde{B} = (\alpha_1, \alpha_2, \alpha_3)(\cdot)(b_1, b_2, b_3) = (\alpha_1 b_1, \alpha_2 b_2, \alpha_3 b_3) \tag{4}$$

$$\tilde{A}(/)\tilde{B} = (\alpha_1, \alpha_2, \alpha_3)(/)(b_1, b_2, b_3) = (\alpha_1 / b_1, \alpha_2 / b_2, \alpha_3 / b_3) \tag{5}$$

2.2 Linguistic Variables

Linguistic variable is a variable that is represented in linguistic terms, i.e words sentences, etc, and whose value can be modeled by a fuzzy set [12]. The concept of linguistic variables can be very useful in dealing with complex or poorly defined to be reasonably described in conventional quantitative expressions evaluation problems. In this paper the importance weights of various criteria and the ratings of qualitative criteria are expressed linguistic variables. These linguistic variables are shown in Table 1.

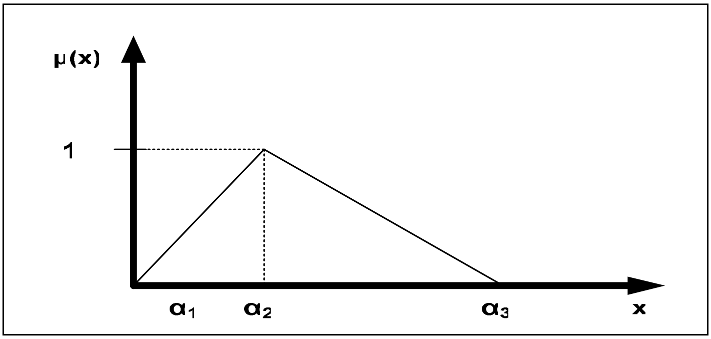


Fig. 1. Triangular fuzzy number

Table 1. Linguistic variables

Very Low (VL)	(0, 0, 0.2)
Low (L)	(0, 0.2, 0.4)
Medium (M)	(0.2, 0.4, 0.6)
High (H)	(0.4, 0.6, 0.8)
Very High (VH)	(0.6, 0.8, 1)
Excellent (E)	(0.8, 1, 1)

3 Multi-Attribute Decision Making (MADM) Methods

3.1 The AHP Method

The Analytic Hierarchy Process (AHP) method was introduced by Saaty [13] with goal the making of decisions about complicated problems by dividing such problems into a hierarchy of decision factors which are simple and easy to analyze. It consists of the following steps:

Step 1- *Determination of the objective and the decision factors*: During this step the final objective of the problem is analyzed as a number of decision factors, which are also further analyzed until the problem acquires a hierarchical structure, in the lowest level of which the alternative solutions of the problem are found.

Step 2- *Determination of the relative importance of the decision factors with respect to the objective:* During this step, in each level the decision factors are compared pairwise according to their levels of influence with respect to the scale shown in Table 2.

The comparison results are presented in a square matrix $A=[\alpha_{ij}]_{n\times n}$ where n are the number of factors, and $\alpha_{ii}=1,\alpha_{ji}=1/\alpha_{ij},\alpha_{ij}\neq 0$.

Table 2. Scale of Importance

Intensity of importance	**Definition**
1	Equal importance
3	Moderate importance
5	Strong importance
7	Very strong importance
9	Extreme importance
2,4,6,8	Intermediate values

Step 3-*Normalization and Calculation of the relative weights:* The relative weights are calculated by finding the right eigenvector (w) corresponding to the largest eigenvalue ($\lambda_{\max}$), as

$$A_w=\lambda_{\max}w \tag{6}$$

In order to avoid potential comparative inconsistency within pairs of categories, a Consistency Index (CI) is defined as

$$CI=\frac{(\lambda_{\max}-n)}{n-1} \tag{7}$$

The Consistency Ratio (CR) is calculated by dividing the CI by the Random consistency Index (RI), and is given by

$$CR=\frac{CI}{RI} \tag{8}$$

If the value of CR is smaller or equal to 10%, the inconsistency is acceptable; otherwise the subjective judgment is revised.

3.2 The Fuzzy TOPSIS Method

The Total Order Preference by Similarity to the Ideal Solution (TOPSIS) method was first introduced by Hwang and Yoon [14], and it is based on the idea that the best alternative should have the shortest distance from the positive ideal solution and farthest distance from the negative ideal solution. In our approach the fuzzy TOPSIS is adopted in order evaluate the candidate networks by using linguistic values.

The Fuzzy TOPSIS method consists of the following steps:

Step 1- *Construction of the fuzzy decision matrix*: The Decision Matrix is expressed as

$$\tilde{D} = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_n \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \cdots & C_m \end{array} \\ \begin{bmatrix} \tilde{d}_{11} & \tilde{d}_{12} & \cdots & \tilde{d}_{1m} \\ \tilde{d}_{21} & \tilde{d}_{22} & \cdots & \tilde{d}_{2m} \\ \vdots & \vdots & \cdots & \vdots \\ \tilde{d}_{n1} & \tilde{d}_{n2} & \cdots & \tilde{d}_{nm} \end{bmatrix} \end{array} \tag{9}$$

where $A_1, A_2, \ldots, A_n$ are the possible alternatives and $C_1, C_2, \ldots, C_n$ are the criteria, which measure the performance of the alternatives. Each element $\tilde{d}_{ij}$ of the fuzzy decision matrix $\tilde{D}$ is the linguistic value of the alternative A_i with respect to the criterion C_j. It should be noted that since the fuzzy linguistic rating $\tilde{d}_{ij}$ preserves the property that the ranges of normalized triangular fuzzy numbers belong to [0,1]; there is no need for normalization.

Step 2- *Construction of the weighted normalized fuzzy decision matrix:* The weighted normalized fuzzy decision matrix is constructed by multiplying each element $\tilde{r}_{ij}$ with its associated weight w_j

$$\tilde{u}_{ij} = \tilde{r}_{ij} w_j \tag{10}$$

Step 3- *Determination of the Fuzzy Positive-Ideal Solution (FPIS) and Fuzzy Negative-Ideal solution (FNIS):* The positive and negative ideal solutions, FPIS A^+ and FNIS A^- respectively, can be defined as:

$$A^+ = \left(\tilde{u}_1^+, \tilde{u}_2^+, \ldots, \tilde{u}_n^+\right) \tag{11}$$

and

$$A^- = \left(\tilde{u}_1^-, \tilde{u}_2^-, \ldots, \tilde{u}_n^-\right) \tag{12}$$

Step 4- *Measurement of the distance of each alternative from FPIS and FNIS:* The distance of each alternative from the ideal and the negative ideal solution is given

$$S_i^+ = \sum_{i=1}^{n} d\left(\tilde{u}_{ij}, \tilde{u}_j^+\right),, j = \{1, \ldots, m\} \tag{13}$$

$$S_i^- = \sum_{i=1}^{n} d\left(\tilde{u}_{ij}, \tilde{u}_j^-\right),, j = \{1, \ldots, m\} \tag{14}$$

Step 5- *Relative Closeness Calculation:* The relative closeness is defined to determine the relative closeness of each alternative $A_i (i = 1,2,\cdots,n)$ from the ideal solution. It is expressed as

$$C_i = \frac{S_i^-}{S_i^- + S_i^+} \left(i = 1,2,\ldots,n\right) \tag{15}$$

Step 6: *Preference Order Ranking:* The best alternatives are ranked according to the C_i value in descending order.

4 Numerical Results

In order to demonstrate how the previously described methods can be utilized for the access network selection, we consider a heterogeneous wireless network that is composed by a Universal Mobile Telecommunications System (UMTS) network, a Worldwide Interoperability for Microwave Access (WiMAX) network and two Wireless Local Area Networks (WLANs), employing the IEEE 802.11b (WLAN1) and IEEE 802.11g (WLAN2) technologies (Figure 2).

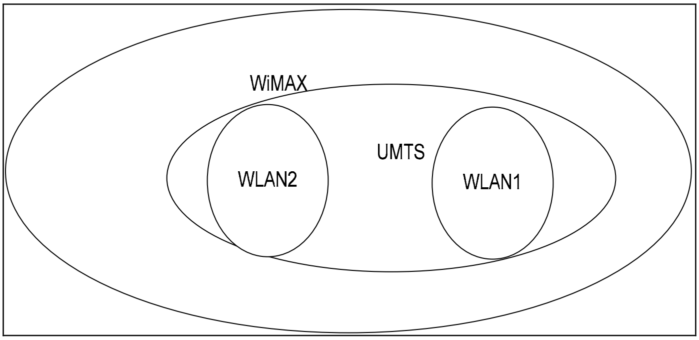


Fig. 2. The Network Topology

We focus our attention on the case that the decision for the network selection is influenced by the requested application indicated by the user. Thus, we consider three applications that are very often used by users, namely VoIP, media streaming and web browsing. In order to determine the importance of the network parameters in these applications, the AHP method is applied. Tables 3 and 4 present the pairwise comparison matrices for the VoIP applications that were formed using the scale of importance of Table 1, while Tables 5 and 6 present the pairwise comparison matrices for the streaming media and the web browsing applications, respectively. The results obtained from the computations based on the pairwise comparison matrices are presented in Figure 3.

Table 3. The pairwise comparison matrix for the basic network parameters for VoIP Applications

VoIP	Throughput	Latency	Reliability	Cost	Security	Weight
Throughput	1	1/5	1/5	1/3	5	0.0937
Latency	5	1	3	3	5	0.3455
Packet Loss	5	1/3	1	5	5	0.3608
Cost	3	1/3	1/5	1	5	0.1564
Security	1/5	1/5	1/5	1/5	1	0.0436

Table 4. The pairwise comparison matrix for the network latency sub-parameters for VoIP Applications

	Delay	Jitter	Weight
Delay	1	1	0.5
Jitter	1	1	0.5

Table 5. The pairwise comparison matrix for the basic network parameters for Streaming Media Applications

Streaming Media	Throughput	Latency	Reliability	Cost	Security	Weight
Throughput	1	5	3	3	5	0.4506
Latency	1/5	1	1	1/3	5	0.1196
Packet Loss	1/3	1	1	1/3	5	0.1308
Cost	1/3	3	3	1	5	0.2554
Security	1/5	1/5	1/5	1/5	1	0.0436

Table 6. The pairwise comparison matrix for the basic network parameters for Web Streaming Applications

Web browsing	Throughput	Latency	Reliability	Cost	Security	Weight
Throughput	1	5	3	1	5	0.3705
Latency	1/5	1	1	1/3	5	0.1264
Packet Loss	1/3	1	1	1/3	5	0.1358
Cost	1	3	3	1	5	0.3226
Security	1/5	1/5	1/5	1/5	1	0.0447

Since the weights of the criteria were determined, then the fuzzy TOPSIS is applied in order to rank the alternative networks. More specifically, during the first step the fuzzy decision matrix (Table 7) is established by the evaluation of alternative networks using the linguistic variables of Table 1. The linguistic variables are in the first line of each row of Table 7, while the second line represents the triangular fuzzy number which is equivalent of the respective linguistic variable.

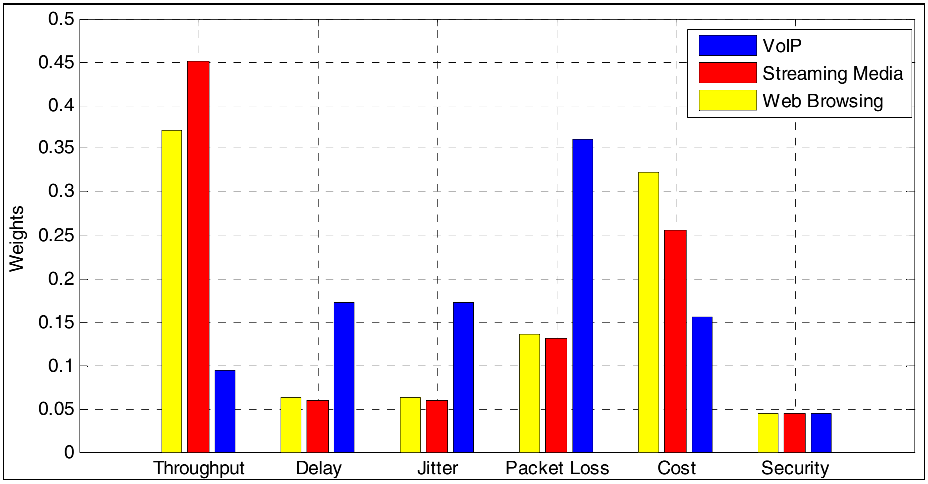


Fig. 3. Weights associated with attributes for different applications

After the fuzzy decision matrix was determined, the fuzzy weighted decision table is constructed by using the criteria weights calculated by AHP (Figure 3). Then, we define the fuzzy positive and negative ideal solutions FPIS A^+ and FNIS A^- as $\tilde{u}_j^+ = (1,1,1)$ for benefit criterion, and as $\tilde{u}_j^- = (0,0,0)$ for cost criterion. Afterwards, the distance of each alternative from the ideal and the negative ideal solutions for each application is computed. Finally, the ranking of each access network for the three applications considered in this work is depicted in Figure 4.

Table 7. Fuzzy evaluation matrix for the alternative networks

Networks	Throughput (Mbps)	Delay (ms)	Jitter (ms)	Packet Loss (%)	Cost (price)	Security (degree)
UMTS	VL (0, 0.2, 0.4)	M (0.2, 0.4, 0.6)	M (0.2, 0.4, 0.6)	H (0.4, 0.6, 0.8)	H (0.4, 0.6, 0.8)	H (0.4, 0.6, 0.8)
WiMAX	E (0.8, 1, 1)	M (0.2, 0.4, 0.6)	M (0.2, 0.4, 0.6)	H (0.4, 0.6, 0.8)	M (0.2, 0.4, 0.6)	M (0.2, 0.4, 0.6)
WLAN1	M (0.2, 0.4, 0.6)	H (0.4, 0.6, 0.8)	M (0.2, 0.4, 0.6)	M (0.2, 0.4, 0.6)	L (0, 0.2, 0.4)	L (0, 0.2, 0.4)
WLAN2	E (0.8, 1, 1)	H (0.4, 0.6, 0.8)	H (0.4, 0.6, 0.8)	M (0.2, 0.4, 0.6)	L (0, 0.2, 0.4)	L (0, 0.2, 0.4)

Table 8. Distances from FPIS and FNIS for each application

	VoIP	Streaming	Web browsing		VoIP	Streaming	Web browsing
S^+	2,240738	2,347383	2,426126	S^-	3,661741	3,562669	3,606211
	1,915713	1,975779	2,336375		3,952175	3,899124	3,69291
	2,053605	2,242848	2,33227		3,821002	3,639801	3,706624
	1,866785	2,012137	2,315001		3,995848	3,855861	3,719506

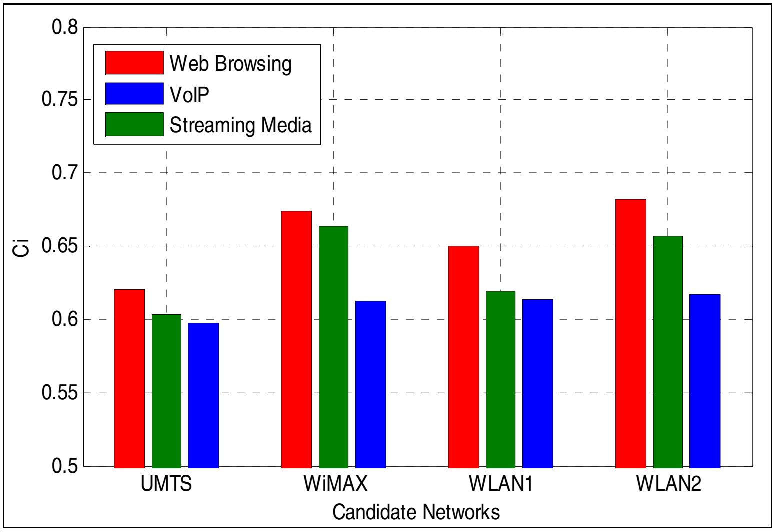


Fig. 4. Results obtained from the fuzzy TOPSIS algorithm for each application

5 Conclusions

Ubiquitous service delivery requires the selection of the optimal access network in a heterogeneous wireless environment. The MADM methods provide an effective framework for ranking the candidate networks in a heterogeneous wireless environment by means of their ratings with respect to multiple attributes. In this paper, an access network selection algorithm for heterogeneous wireless networks is proposed that combines two MADM methods, the AHP method to determine the importance of the network parameters and the TOPSIS method to rank the candidate networks. The novelty of the proposed approach is that instead of applying fuzziness during the determination of the weights, the fuzziness is applied during the ranking of the candidate networks, since it is more precise to determine the level of influence of the criteria than to characterize the value of a criterion. Numerical results showed that the combination of these two methods can be very effective for the selection of the optimal access network according to requirements of the application that the user wishes to utilize.

Future work includes evaluating the efficiency of the proposed access network selection algorithms during vertical handoffs in heterogeneous environments since the computational complexity is minimal. Moreover, we are targeting at taking into account additional criteria for the optimal network selection such as availability of network resources, Received Signal Strength (RSS) and Signal-to-Noise Ratio (SNR).

References

1. Song, Q., Jamalipour, A.: Quality of Service Provisioning in Wireless LAN/UMTS Integrated Systems Using Analytic Hierarchy Process and Grey Relational Analysis. In: 47th annual IEEE Global Telecommunications Conference (GLOBECOM 2004), pp. 220–224. IEEE, Dallas (2004)

2. Alexandri, E., Martinez, G., Zeghlache, D.: Adaptive Joint Call Admission Control and Access Network Selection for Multimedia Wireless Systems. In: 5th International Symposium Wireless Personal Multimedia Communications, pp. 1390–1394. IEEE, Honolulu (2002)
3. Skianis, C., Kormentzas, G., Kontovasillis, K.: Interactions between intelligent multimodal terminals and a network management system in a B3G Context, Special Issue on WLAN/3G Integration for Next-Generation Heterogeneous Networks. Wireless Communications and Mobile Computing 5, 679–695 (2005)
4. Bari, F., Leung, V.: Application of ELECTRE to Network Selection in A Hetereogeneous Wireless Network Environment. In: The 2007 IEEE Wireless Communications and Networking Conference (WCNC 2007), pp. 3810–3815. IEEE, Syndney (2007)
5. Bari, F., Leung, V.: Automated Network Automated network selection in a heterogeneous wireless network environment. IEEE Network 21(1), 34–40 (2007)
6. Song, Q., Jamalipour, A.: Network Selection in an integrated Wireless LAN and UMTS Environment Using Mathematical Modeling and Computing Techniques. IEEE Wireless Communications 12(3), 42–48 (2005)
7. Wu, J.S., Yang., S.F., Hwang, B.J.: A Terminal-Controlled Vertical Handover Decision Scheme in IEEE 802.21-Enabled Heterogeneous Wireless Networks. International Journal of Communication Systems 22, 819–834 (2009)
8. Charilas, D.E., Markaki, O.I., Psarras, J., Constantinou, P.: Application of Fuzzy AHP and ELECTRE to Network Selection. In: 1st International Conference on Mobile Lightweight Wireless Systems (Mobilight 2009), Athens, Greece, May 18-20 (2009)
9. Dagdeviren, M., Yavuz, S., Kılınç, N.: Weapon selection using the AHP and TOPSIS methods under fuzzy environment. Expert Systems with Applications 36, 8143–8151 (2009)
10. Zadeh, L.A.: Fuzzy sets. Inf. Control 8, 338–353 (1965)
11. Dweiri, F.: Fuzzy development of crisp activity relationship charts for facilities layout. Computers and Industrial Engineering 36, 1–16 (1999)
12. Zimmermann, H.J.: Fuzzy set theory and its applications. Kluwer, Boston (1991)
13. Saaty, T.L.: The Analytic Hierarchy Process. RWS Publications, Pittsburgh (1990)
14. Hwang, C.L., Yoon, K.: Multiple attribute decision making: Methods and applications, A State of the Art Survey. Springer, New York (1981)

Adaptive Message Ferry Route (aMFR) for Partitioned MANETs

Ting Wang and Chor Ping Low

School of Electrical and Electronic Engineering,
Nanyang Technological University, Singapore
{wang0235,icplow}@ntu.edu.sg

Abstract. *Message ferrying (MF)* scheme is a scheme to restore a *Mobile Ad Hoc Network (MANET)* from partitioning. Despite of effectiveness, it suffers from long delay caused by the poor design of ferry route. The *Message Ferry Route (MFR)* problem has been studied to minimize this drawback of MF schemes. In this paper, we argue that an adaptive way of constructing the ferry route would be more practical and effective. We thus define the *Adaptive MFR (aMFR)* problem with more general and realistic assumptions, and propose a new scheme for adaptive message ferrying. The proposed scheme adopts the *Shortest Process Time First (SPTF)* rule for the *Job Sequencing Problem (JSP)*, to construct ferry routes and is referred to as *AMFeR*. From simulations, we show that AMFeR can shorten the average message delay. With its simplicity and distributed nature, AMFeR is a suitable solution for partition restoration of MANETs.

Keywords: Mobile Ad Hoc Network (MANET), Message Ferry, Ferry Route, Message Delay.

1 Introduction

A *Mobile Ad Hoc Network* (MANET) is a kind of mobile wireless network, which is a collection of mobile hosts connected through wireless channels. The hosts of a MANET are usually called *nodes* while direct connections between the nodes are referred to as *links*. A node in a MANET exchanges messages with other nodes as a terminal and forwards the messages as an intermediate routers at the same time. The routing path of a message in a MANET is formed by a collection of mobile nodes. Messages are forwarded hop by hop.

While mobility of nodes enables the network to span over a large area, it also causes a highly dynamic topology, which is a major challenge in the applications of MANETs. When a node moves out of another's communication range, the link between them breaks. The entire message routing path may be destroyed by this broken link. This possibility of link breakage may split nodes into parts (components) between which no possible path exists. This in turn may result in packets not being able to reach their destinations. We refer this phenomenon as *network partitioning*. Each isolated component of a network is referred to as a

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 99–111, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

partition of the network. The partitioning problem makes a critical strike on ad hoc routing because most protocols typically assume that the network is always connected. To enhance the reliability and conserve energy, partitioning should be prevented in MANETs.

Various approaches have been proposed in recent years for the MANET survivability and restoration. One of them, namely the *Message Ferrying (MF)* scheme [10], uses special nodes as *ferries* to deliver messages across partitions of a MANET. With MF scheme, despite the fact that the nodes in a MANET are partitioned, the ferries restore the connection by moving from one partition to another. However, ferries' movement consumes considerable amount of energy and time, causing long message delay in the network. These drawbacks of MF scheme can be minimized by optimizing the route on which each ferry moves. In [10] Zhao *et al.* formulated the *Massage Ferry Route (MFR)* problem and adapted solutions from the well studied *Traveling Salesman Problem (TSP)*. In [8], inter arrival times of areas are used to construct the ferry routes. In all these works, the ferry does not change its route when it moves in the network, making its route static. We will show in this paper why such a static solution of MFR will not be optimal and an adaptive scheme would be preferred.

Some other existing works such as [5] do consider the destination of each message when constructing the ferry routes. However, the location and movement information, such as coordinates, speed and directions of other nodes are needed to construct the ferry routes. This need of collaboration between nodes and ferries makes these schemes costly in energy consumption and bandwidth usage. Moreover, under the assumption that the network is partitioned, such information may not be available to the ferries. Thus, the route could not be determined effectively. Hence, localized schemes would be preferable.

In this paper we redefine the MFR problem in an adaptive context, as a new problem referred to as the *Adaptive Message Ferry Route (aMFR)* problem. A new scheme, namely *AMFeR* is also proposed for this problem. As opposed to the existing schemes, AMFeR is adaptive in the sense that it only decides the next segment of the route based on the traffic in the network. We adpot the *Shortest Process Time First (SPTF)* rule from the *Job Sequencing Problem (JSP)* and define a selection factor to construct the ferry route. This allows a ferry to change its route adaptively in respond to the traffic. Moreover, AMFeR is a fully localized scheme that does not incur any additional communication among nodes in the network. Our simulation shows that AMFeR can effectively shorten the average message delay in the network as compared to existing schemes.

The remaining parts of this paper is organized as follows. Section 2 states the assumptions we make in this work and defines the aMFR problem. In Section 3, we describe our observations concerning the aMFR problem. These observations lead us to our solution to the problem, namely the AMFeR scheme, which will be introduced in Section 4. Our simulation results are discussed in Section 5. Finally, we conclude this paper with Section 6.

2 Problem Formulation

The route of a ferry in MF scheme is usually defined by a series of points referred to as *waypoints*. The ferry stops on each of these waypoints and moves towards the next one according to a given sequence. The line segment connecting each pair of consecutive waypoints is referred to as a *leg* of the route. In most of the existing works, the sequence of waypoints does not change its order once being constructed, and is thus referred to as a *static route*. Moreover, since the solution of TSP is usually adapted for route construction, the route is a *cycle* in the topology graph, where no waypoint repeats. The time needed to finish one cycle of the static route is the *length* of the route.

In this paper, we aim to construct an *adaptive route* for the ferry. It is adaptive because the sequence of waypoints changes over time according to the messages being transmitted in the network. Also, we allow the route to be a *walk* instead of a cycle, where waypoints may repeat. In this section, we discuss the assumptions and notations used in this paper, and then define the *adaptive Message Ferry Route (aMFR)* problem.

2.1 Assumptions and Notations

The original *Message Ferry Route (MFR)* problem is defined in [10] with two fundamental assumptions:

- the nodes are stationary and their positions are known to the ferry;
- the traffic between two given nodes can be estimated prior to constructing the ferry route.

These assumptions can hardly be met in a typical MANET, where nodes move around and the traffic can hardly be predicted. Therefore, in this paper, we target to consider a more practical scenario, where:

- the nodes are mobile;
- the traffic in the network is randomly variant and is thus not predictable.

The MANET of our interest has n mobile nodes and f ferries. We assume the network is partitioned to k components, each of which forms a *cluster* with a chosen *Cluster Head (CH)*. In order to simplify the problem, we restrict the movement of a *CH* inside a circular area, namely the *Head Zone (HZ)*. The radius of *HZ* equals to the communication range of the nodes, denoted as r, as shown in Fig. 1. The center of *HZ* of cluster i is denoted as point C_i, $1 \leq i \leq k$. We use ϵ_{ij} to denote the time taken by a ferry to travel from C_i to C_j, $1 \leq i, j \leq k$. We note that ϵ_{ij} is a positive real number. We say cluster i and j are *neighbors* unless $\epsilon_{ij} = \infty$, which means the ferry cannot move directly from cluster i to cluster j.

We assume the movements, splitting and combinations of the clusters are all handled by some clustering scheme so that the *CH* is aware of any change of the cluster members, *i.e.* *CH* works as a proxy between the cluster members and the

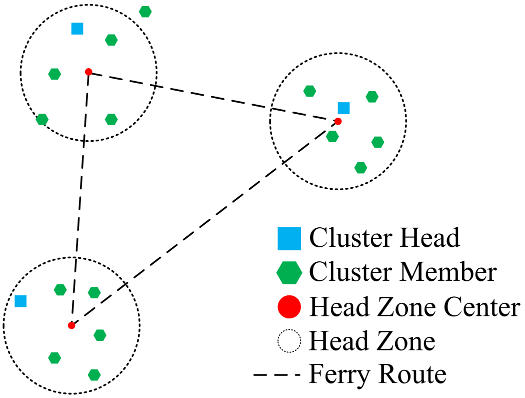


Fig. 1. Network Topology

ferry. There are many existing clustering schemes which can be adopted, such as [9], for this purpose.

By the above definitions and assumptions, if a ferry stops at C_i, it is able to communicate with the *CH* of cluster i. The ferry only need to communicate with *CH*s to deliver the messages to other nodes. The route of ferry, denoted as $\mathbb{R}$, will be a sequence of *HZ* centers (C_i's), each of which is equivalent as a waypoint.

Moreover, since nodes in the same cluster are connected, we can use normal MANET routing protocols such as AODV or DSR for the communication between a CH and its members. We note that the delay incurred by the message transmission within a cluster (*intra-cluster communication*) is much smaller than between different clusters (*inter-cluster communication*), and is also less relevant to the ferry route. As a consequence, intra-cluster communication will be omitted in our following discussion.

2.2 Objective

In [10], the objective function of the original MFR problem is defined to minimize:

$$\Delta^{\mathbb{R}} = \frac{\sum\limits_{1\leq i,j\leq k} b_{ij}\delta_{ij}^{\mathbb{R}}}{\sum\limits_{1\leq i,j\leq k} b_{ij}}, \qquad (1)$$

where b_{ij} is the average traffic from i to j, and $\delta_{i,j}^{\mathbb{R}}$ is the time spent by the ferry to travel from i to j on the static route $\mathbb{R}$. $\Delta^{\mathbb{R}}$ is thus the weighted average of delay incurred by route $\mathbb{R}$. We note that $\delta_{i,j}^{\mathbb{R}}$ is the time spent on traveling on the route, and thus $\Delta^{\mathbb{R}}$ is referred to as the *traveling delay* on route $\mathbb{R}$.

We should also note that before the messages are collected by the ferry, they need to wait at their sources for certain amount of time. This kind of delay is not counted in the traveling delay. We refer to this amount of time spent on waiting at source as the *waiting delay.*

The waiting delay is not taken into account in the objective function of MFR. This is because for a static route, waiting delay is always bounded from above by the length of route $\mathbb{R}$, denoted as $\delta^{\mathbb{R}}$. If the traffic is uniform, the expected value of waiting delay is fixed at $\delta^{\mathbb{R}}/2$.

However, since we have assumed that the traffic is not uniform and unpredictable, b_{ij} could not be determined beforehand. We could not use Eqn. 1 to measure the delay under our new assumptions to the aMFR problem. In addition, because we use an adaptive route, the length of the route is not fixed. This in turn imply that the upper bound and the average value of the waiting delay for a static route is not applicable in this case. Due to these facts, we need to measure the delay for each message to compute the overall delay.

Assume within time duration $(0, t]$, there are m messages to be transmitted by the ferries. The size of message h $(1 \leq h \leq m)$ is μ_h, and its source and destination cluster are denoted as s_h and d_h respectively. The *delay* (δ_h) of the message h is comprised of two parts, namely *waiting delay* (ω_h) and *traveling delay* (τ_h).

After the *CH* receives messages from other cluster members, it needs to firstly wait for a ferry to come in contact with it. This amount of time spent for waiting the ferry is ω_h. The *weighted average waiting delay* (Δ_ω) of all the messages is given by

$$\Delta_\omega = \frac{\sum\limits_{h=1}^{m} \mu_h \omega_h}{\sum\limits_{h=1}^{m} \mu_h}. \tag{2}$$

Next, the ferry will move from C_{s_h} to C_{d_h} on its chosen route, incurring the traveling delay τ_h. However, since the route adapts to traffic and changes dynamically, τ_h may not be equal to τ_g, for any two given messages h and g which have the same source and same destination. The *weighted average traveling delay* (Δ_τ) of all the messages is taken as

$$\Delta_\tau = \frac{\sum\limits_{h=1}^{m} \mu_h \tau_h}{\sum\limits_{h=1}^{m} \mu_h}. \tag{3}$$

The overall delay of message h, $\delta_h = \omega_h + \tau_h$. The *weighted average overall delay* of the messages is thus

$$\Delta = \frac{\sum\limits_{h=1}^{m} \mu_h \delta_h}{\sum\limits_{h=1}^{m} \mu_h} = \frac{\sum\limits_{h=1}^{m} \mu_h \left(\omega_h + \tau_h\right)}{\sum\limits_{h=1}^{m} \mu_h} = \Delta_\omega + \Delta_\tau. \tag{4}$$

The objective of aMFR problem is to find an adaptive route with C_i as waypoints to minimize Δ.

3 Observations

We could make the following observations from the aMFR problem:

- **It's infeasible to find the optimal adaptive ferry route in the aMFR problem.** The complexity of the aMFR problem can be reduced when we only consider Δ_ω or Δ_τ. When we neglect the waiting delay and assume that only one cluster transmits messages, the aMFR problem can be reduced to the weighted *Minimum Latency Problem (MLP)*, which is known to be a MAX-SNP-hard problem [4]. Generally, there is no polynomial time approximation scheme for MAX-SNP-hard problems [1]. Even for a more simplified scenario, where μ_i is constant and the traffic is uniform among the clusters, the problem reduces to the *Traveling Salesman Problem (TSP)*, which is still NP-hard. On the other hand, if we neglect the traveling delay and consider only the waiting delay, the problem is in fact still a NP-hard variation of TSP, namely *Prize Collecting TSP (PCTSP)* [3]. Therefore, it is highly unlikely that we could construct an optimal adaptive ferry route in polynomial time.
- **A static route can not be the optimal solution.** This is because in the network, traffic may not be constant and uniform all the time. If some cluster i receives messages more frequently than others, it will be a waste of time to visit all the other clusters before returning to cluster i, which is what will take place with a static route. Moreover, due to the nature of the MANET tasks, such as area exploration or surveillance, the frequency and sizes of messages may vary over time. A static route could not adapt itself to such changes.
- **The key to finding a suitable route is to determine the *next leg*.** The ferry stops to deliver and collect messages to/from a CH after each leg. Therefore, we do not need to plan the route beyond the next leg, as the future legs should be dynamically determined according to the messages that a ferry will collect in the future and are not unveiled to the ferry yet. Therefore, if a scheme can produce the next leg effectively, it will offer a good solution to the aMFR problem.

Based on the above observations, we propose to use a new scheme namely AMFeR to choose the "best"[1] *CH* among all the neighbors as the next waypoint of the ferry to form the dynamic ferry route.

4 The AMFeR Scheme

4.1 JSP and the SPTF Rule

In the *Job Sequencing Problem (JSP)* [2] of a single machine, we need to find the optimal sequence of a series of jobs j with weight[2] l_j and process time p_j to minimize the average delay of these jobs given by:

---

[1] As the most suitable waypoint in a adaptive ferry route to minimize Δ.

[2] Larger l_j represents higher importance and vice versa.

$$\varDelta_{\mathrm{jsp}} = \frac{\sum_j l_j \delta_j}{\sum_j l_j} \tag{5}$$

Smith proved in [7] that the optimal solution to JSP can be produced by following the *Shortest Process Time First (SPTF)* rule:

- **SPTF Rule:** Sequencing the jobs in order of non-decreasing ratio p_j/l_j produces an optimal schedule to minimize $\varDelta_{\mathrm{jsp}}$.

Comparing Eqn. 5 with Eqns. 2, 3 and 4, we can observe that the objective functions in JSP and aMFR are similar (details will be discussd in the next Section). Hence SPTF would be a useful tool in constructing adaptive ferry route. In this paper, to ensure that the equations that we derive in the next Section are well defined, we define an *inverse SPTF (iSPTF)* rule:

- **iSPTF Rule:** To optimally sequence the jobs in JSP, the job with *highest* l_j/p_j value should be chosen first.

It is easy to see that iSPTF is logically equivalent to SPTF. They are both able to solve JSP optimally.

4.2 AMFeR

In the aMFR problem, we may interpret the event that the ferry goes to a destination cluster j as job j. Assuming the ferry is currently at cluster i, we could say that the required processing time of job j is the traveling time from cluster i to cluster j, *i.e.* ϵ_{ij}, which is similar to p_j in the JSP.

In order to apply the iSPTF rule, we need to determine the weight l_j of these jobs. We note in JSP, the weight of a job indicates the how much each job contributes to the objective function $\varDelta_{\mathrm{jsp}}$. In contrast, job j contributes in both $\varDelta_\omega$ and $\varDelta_\tau$ in the aMFR problem.

The contribution of job j to $\varDelta_\omega$ is based on the size of the messages that a ferry collects when it visit cluster j. We define the total size of these messages as $M_{s=j}$. On the other hand, job j also contributes to $\varDelta_\tau$ by delivering the messages with destinations in cluster j. We denote the total size of messages delivered by the ferry in job j is denoted as $M_{d=j}$. Therefore, the overall contribution of job j to the objective function $\varDelta$ is $M_{s=j} + M_{d=j}$. We use this value as the weight of job j (like l_j in JSP). Then we can choose the cluster with maximal ratio of $\left(M_{s=j} + M_{d=j}\right)/\epsilon_{ij}$ as the next waypoint of the adaptive route according to the iSPTF rule.

We also note that the aMFR problem and JSP are still two different problems. This is due to the fact that in the aMFR problem, ϵ_{ij} varies with the ferry's location (cluster i), while in JSP p_j is constant. Therefore iSPTF may not provide the exact optimal solution to the aMFR problem. However, since we are not interested in the entire route but the next leg, we believe the iSPTF rule still provides a good indication of which cluster should be the next waypoint.

Table 1. Algorithm for AMFeR

```
arrive(cluster $i$, time $\Phi$){
  initialize $\mathcal{F}_j$, $M_{s=j}$ and $M_\tau$ to 0 for all $j$
  deliver messages to cluster $i$
  for each message $h$ collected from cluster $i$ do          %Step 1%
    store message $h$
    compute $M'_{s=i} += \mu_h$
  for each undelivered message $h$ do                          %Step 2%
    compute $M_{d=d_h} += \mu_h$
  for each cluster $j$ do                                      %Step 3%
    compute $M_{s=j} = \frac{{M'}_{s=j}}{\phi_j}(\Phi + \epsilon_{ij} - \phi_j)$
    compute $\mathcal{F}_j = \frac{M_{s=j} + M_{d=j}}{\epsilon_{ij}}$
  for all the clusters do                                      %Step 4%
    find $j_{max}$ of which $\mathcal{F}_{j_{max}}$ is the maximum
  arbitrarily break ties
  set $\phi_i = \Phi$
  move to the next waypoint $C_{j_{max}}$
}
```

We still need to compute $M_{s=j}$ and $M_{d=j}$. $M_{d=j}$ depends only on the messages collected by the ferry and not yet be delivered, *i.e.* the stored messages. The ferry can find the exact value of $M_{d=j}$ by going through its storage to calculate

$$M_{d=j} = \sum_{h|d_h=j} \mu_h, \tag{6}$$

where h is the id of the message.

However, $M_{s=j}$ is unveiled only after the ferry has arrived at cluster j. Hence we have to project its value. We use Φ to denote the current time and ϕ_j as the time of the most recent arrival of the ferry at cluster j ($\phi_j < \Phi$). The total size of messages previously sent from cluster j is denoted as $M'_{s=j}$. The average data rate during $(0, \phi_j]$ is thus $\frac{M'_{s=j}}{\phi_j}$. If the ferry goes from cluster i to cluster j in the next leg, it will arrive at C_j at time $\Phi + \epsilon_{ij}$. The messages waiting at cluster j are accumulated from time ϕ_j to $(\Phi + \epsilon_{ij})$. Their total size is predicted as

$$M_{s=j} = \frac{{M'}_{s=j}}{\phi_j}\left(\Phi + \epsilon_{ij} - \phi_j\right). \tag{7}$$

Using Eqns. 6 and 7, we can define a *selection factor* $\mathcal{F}$ as

$$\mathcal{F}_j = \frac{M_{s=j} + M_{d=j}}{\epsilon_{ij}} = \frac{\sum\limits_{h|d_h=j} \mu_h + \frac{M'_{s=j}}{\phi_j}\left(\Phi + \epsilon_{ij} - \phi_j\right)}{\epsilon_{ij}} \tag{8}$$

for each cluster j. Cluster with maximal $\mathcal{F}_j$ will be chosen as the next waypoint of the route by iSPTF rule. Ties can be broken arbitrarily.

Lemma 1. *The complexity of algorithm* `arrive` *is* $O(k+m)$.

Proof. Step 1 in `arrive` updates the collected messages size $M'_{s=i}$ of current cluster (cluster i). Since the total number of messages is m, Step 1 takes $O(m)$ time in the worst case. In Step 2, the algorithm goes through the ferry's storage to calculate the accumulated size of messages $M_{d=d_h}$ that will be delivered to cluster d_h. This also takes at most $O(m)$ time. In Step 3, the projected size of messages $M_{s=j}$ waiting at each cluster is calculated. It will takes $O(k)$ time. To find the maximal selection factor $\mathcal{F}_j$ in Step 4, another $O(k)$ time is required. The overall complexity for algorithm `arrive` is thus $O(k+m)$. □

We note the complexity of algorithm `arrive` is much lower than almost all the known TSP schemes. Moreover, being a fully localized scheme, AMFeR is very suitable to the MANETs where the resources are limited.

5 Simulations Results

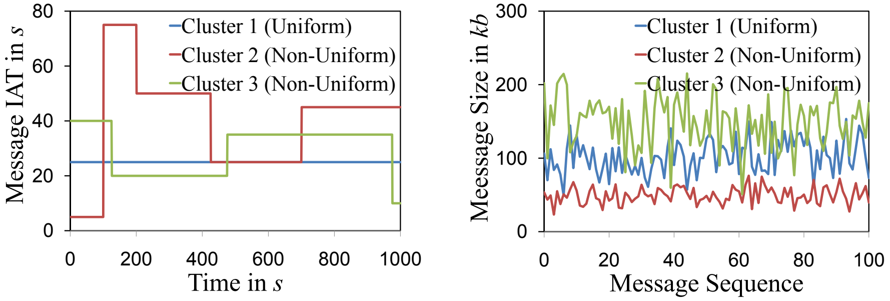
In the simulations, we randomly generate the network topology and traffic to test the effectiveness of AMFeR and compare with existing MFR solutions, namely TSP route and approximate TSP route.

We model k clusters distributed in a 200m by 200m area. The number of nodes in each cluster is a uniform random integer in the interval $[5,20]$. A group of f ferries are used in the MANET. The communication range of the nodes and the ferries is 5m. We require each pair of *HZ* centers be at least 20m apart to ensure that the network is partitioned. The ferries move at a speed of 10m/s. Ferry routes are constructed using AMFeR and TSP (with *HZ* centers as waypoints).

It is well-known that TSP is a NP-hard problem, where optimal solution can not be found within polynomial time. We use brute force to find the optimal TSP route in the simulation. However it would only be feasible to use approximate TSP route for the ferries in practise. To reflect this fact, we also use the *Improving Search Algorithm* [6] to find an approximate solution to TSP as a feasible route. Both optimal and approximate TSP routes are static and are used as benchmarks to compare with AMFeR.

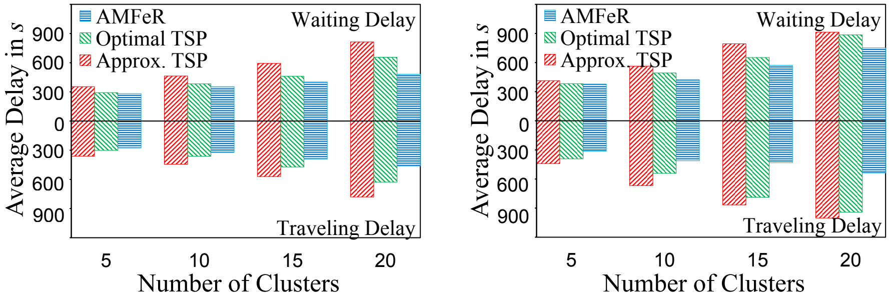
The network traffic can be described by the average size of the messages and the expected time duration between the generation of two consecutive messages at a source. The latter parameter is referred to as the *message inter arrival time*. Since the intra-cluster communication is omitted, we consider each *CH* as a source of the traffic. We use NS-2 to simulate the traffic in the network. Two traffic patterns are considered, namely *uniform traffic* and *non-uniform traffic*.

In uniform traffic pattern, the message inter arrival time fixed at 25sec and and the average size of messages is 100kb for all clusters. However, as we stated in Section 3, uniform traffic may not be realistic for most applications in MANETs. Therefore we use random numbers to control the expected inter arrival time and average size of the messages in non-uniform traffic pattern, as shown in Fig. 2.



(a) Message Inter Arrival Time (b) Message Size

Fig. 2. Traffic Patterns



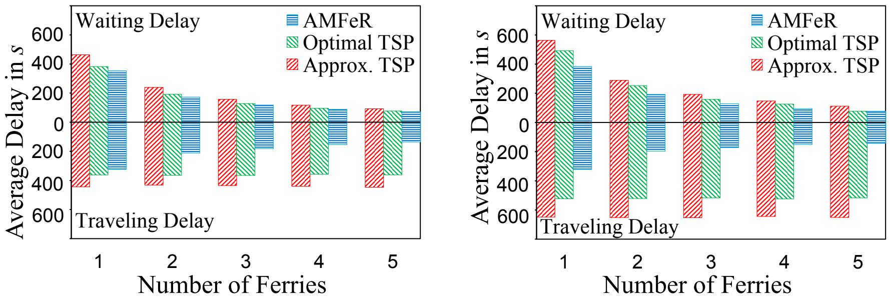
(a) Uniform Traffic (b) Non-Uniform Traffic

Fig. 3. Performance with Different Number of Clusters (k)

Fig. 2(a) depicts the expected message inter arrival time of 3 clusters, one of which has uniform traffic, another two has non-uniform traffic which changes its expected inter arrival time every 25sec with a probability of 0.2.

The values of message size in both traffic patterns are plotted in Fig. 2(b). Cluster 1 represents a cluster with uniform traffic pattern while cluster 2 and 3 are with non-uniform traffic pattern, in which the size of a message is generated using a Gaussian distribution. For each cluster, the mean value of the Gaussian distribution is a random number drawn from the interval $[10\text{kb}, 300\text{kb}]$.

To show the performance of the MFR schemes in different scenarios, we assign different values to k and f. For each scenario, we generate a total number of 10000 messages to calculate their weighted average delay according to Eqns. 2, 3 and 4. The results are plotted in Fig. 3 and 4. In each figure, the results are shown as a group of vertical bars. The upper part of each bar shows the length of average waiting delay Δ_ω, and the lower part corresponds to the traveling delay Δ_τ. As a result, the entire bar length shows the overall average delay Δ of the scheme.



(a) Uniform Traffic (b) Non-Uniform Traffic

Fig. 4. Performance with Different Number of Ferries (f)

Fig. 3 shows the performance of the three ferry route schemes with different numbers of clusters, which increases from 5 to 20. A single ferry is used in these scenarios. For both uniform (Fig. 3(a)) and non-uniform (Fig. 3(b)) traffic, AMFeR outperforms the other two schemes by having much lower average delays. With increasing number of clusters, the ferry may need to stop at more clusters before reaching the destination, which results in longer waiting delay and traveling delay for all the schemes with both traffic patterns. The difference in traveling delay of the schemes are much larger with non-uniform traffic pattern, as shown in Fig. 3(b). This is because in AMFeR the route is generated dynamically according to the traffic and thus shorten the traveling delay. However, the waiting delay of AMFeR also increases to a higher value in the non-uniform traffic scenario as compared to the uniform traffic case. This is because we projected the value of $M_{s=j}$ to construct the route. With non-uniform traffic pattern, this projection will become less accurate, causing a higher waiting delay.

We also vary the number of ferries to obtain Fig. 4. Ferries are randomly allocated at one of the total 10 clusters initially. We note that AMFeR is a fully distributed scheme; so no collaboration is needed among the ferries. Each ferry can decide its route locally. The increase in ferry number does not affect the complexity of AMFeR scheme at all.

From Fig. 4, we can see the ferry number has different impacts on the waiting and traveling delays. The traveling delay drops to a lower value with increasing ferry number only when AMFeR is used. For TSP and approximate TSP routes, no significant change in Δ_τ can be observed. This is because when the same static route is used, the delay of a message only depends on the distance between its source and destination on the route, and is not dependent on the number of ferries. Therefore once the static route is constructed, the traveling delay of messages will not change due to the change in ferry number. On the other hand, when AMFeR is used, the ferries defines their own route based on the messages they are carrying. The traveling delay of a message can be shortened if there are fewer messages carried by the same ferry. Time can be thus saved. As the number of ferries increases, fewer messages will be carried by each of them, and the average traveling delay is thus further decreased.

On the other hand, the waiting delay drops for all 3 schemes when more ferries are deployed in the MANET. This is because even when a static ferry route (TSP or approximate TSP) is used, a cluster can be visited more frequently by the ferries when we use more ferries in the network. The time for which the messages have to wait at the *CH* is thus shortened. More specifically, if the value of waiting delay is Δ_ω when a single ferry is used, the value decreases to approximately Δ_ω/f when f ferries are deployed. Similar result can be observed with AMFeR.

In all the scenarios, the overall delay in AMFeR is significantly lower than other schemes. The results show that ferries using adaptive ferry route deliver the messages faster than those using static route. AMFeR is an effective ferry route scheme in partition restoration in MANETs.

6 Conclusion

In this paper, a problem of constructing message ferry route is addressed. We study the existing Message Ferry Route (MFR) problem and define an adaptive version of the problem (aMFR), which is believed to be more practical to real life applications as compared to the original definition. We propose AMFeR as a solution to the aMFR problem. In AMFeR, we used a similar concept from the Job Sequencing Problem (JSP) and defined a selection factor to construct the ferry route adaptively. From our simulations, we show that AMFeR effectively reduce the overall delay as compared to the existing solutions. Moreover, as AMFeR is a fully distributed scheme with little computation and storage complexity, it is a suitable solution for partition restoration in MANETs.

References

1. Arora, S., Lund, C., Motwani, R., Sudan, M., Szegedy, M.: Proof verification and the hardness of approximation problems. J. ACM 45(3), 501–555 (1998)
2. Baker, K.R.: Introduction to Sequencing and Scheduling. John Wiley & Sons, Inc., Chichester (1974)
3. Balas, E.: The Prize Collecting Traveling Salesman Problem. Networks 16(6), 621–636 (2006)
4. Blum, A., Chalasani, P., Coppersmith, D., Pulleyblank, B., Raghavan, P., Sudan, M.: The Minimum Latency Problem. In: Proceedings of the 26th Annual ACM Symposium on Theory of Computing (STOC 1994), pp. 163–171. ACM, New York (1994)
5. Li, Q., Rus, D.: Communication in Disconnected Ad Hoc Networks Using Message Relay. J. Parallel Distrib. Comput. 63(1), 75–86 (2003)
6. Merz, P., Freisleben, B.: Genetic Local Search for the TSP: New Results. In: Proceedings of the 1997 IEEE International Conference on Evolutionary Computation, pp. 159–164 (April 1997)
7. Smith, W.E.: Various Optimizers for Single-Stage Production. Naval Research Logistics Quarterly 3, 59–66 (1956)

8. Tariq, M.M.B., Ammar, M., Zegura, E.: Message Ferry Route Design for Sparse Ad Hoc Networks with Mobile Nodes. In: Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2006), pp. 37–48. ACM, New York (2006)
9. Zhang, Y., Low, C.P., Ng, J.M., Wang, T.: An Efficient Group Partition Prediction Scheme for MANETs. In: Proceedings of the 2009 IEEE Wireless Communications and Networking Conference (WCNC 2009), pp. 1–6 (2009)
10. Zhao, W., Ammar, M.: Message Ferrying: Proactive Routing in Highly-Partitioned Wireless Ad Hoc Networks. In: Proc. of the Ninth IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS 2003), Washington, DC, USA, pp. 308–314 (2003)

Lightweight Mechanisms for Self-configuring Protocols

Eleni Patouni and Nancy Alonistioti

Department of Informatics & Telecommunications, University of Athens
Athens, Greece
{elenip,nancy}@di.uoa.gr

Abstract. In next generation networks, the introduction of intelligence and flexibility in mobile devices and network nodes appears as a promising solution to the high degree of variability in the telecommunication environment. The materialization of these concepts under the autonomic networking notion paves the way for introduction of awareness and adaptation capabilities in various layers of mobile devices, also including the protocol stack. In this paper we investigate the problem of dynamic protocol stack adaptation and propose enabling mechanisms for the dynamic binding and replacement of their constituent components. Our work addresses the challenge of the application feasibility and performance evaluation of these concepts by quantifying the introduced delay. The obtained results show that the introduced protocol adaptation functionalities pose negligible performance impact in the system. Our work reveals that although flexibility and performance stand on the opposite sides of the system balance, the introduction of transparent mechanisms leads to great adaptability with minimum performance impact.

Keywords: self-configuring, protocol component, reconfiguration, feasibility, lightweight.

1 Introduction

In the heterogeneous environment of next generation networks, the coexistence of various radio access technologies (RATs) and the continuous launch of new and emerging paradigms increase the overall system complexity. At the same time various challenges should be addressed mainly related to the seamless and transparent integration of the new technologies. Such challenges are also tightly coupled with the vast proliferation of the user needs: user requirements impose the philosophy of seamless, anywhere, anytime connectivity and support of multiple types of mobile devices. In this context, one promising solution for addressing such requirements is the introduction of flexibility and intelligence in the system, including both the mobile devices and the network side.

One path in achieving this goal is realised through the emerging visions of reconfigurability and autonomic networking [1],[2] that bring forward new adaptation capabilities in the different layers of the protocol stack and system resources [3]. However, it is often argued that such features increase even more the system complexity. Autonomic networking is viewed as a solution that "fights complexity with complexity" [4]. Practically, this means that the complexity of managing a system is

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 112–123, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

dealt by introducing complex mechanisms in the different system elements that enable them to be aware of the surrounding environment (self-awareness), manage themselves (self-management) and dynamically adapt to the environmental stimuli following high-level objectives and policy rules (self-configuration) [5].

In this direction, this paper addresses the aspect of dynamic adaptation and self-configuration in the protocol stack of mobile devices. In legacy systems, the protocol stack design is driven by the strict performance and resource requirements of mobile devices and network elements. Targeting the fulfilment of such requirements, protocol stack subsystems yield two main principles: a) monolithic, layered design and b) design tightly coupled and statically bound to the networking architecture. The abovementioned design principles lead to platform-dependent implementations that are highly optimized and often tied to the underlying operating system. In such systems, performance is a function of the allocation flexibility offered by the protocol stack's processing model and the minimization of context switches occurring in its operation. In this direction, evolutionary methods for flexible protocol layer design with seamless and transparent adaptation capabilities are necessary to boost the system performance.

Leveraging our previous work in [2],[6] for design of self-configuring protocols, this work focuses on the feasibility and performance evaluation of such concepts. This is realised by introducing the necessary support functionality and signalling between the mobile device and the network side for the realisation of protocol self-configuration. In addition, special focus is paid on the performance evaluation of these mechanisms in the mobile device. In order to test the feasibility of the proposed solution, there is a need to evaluate whether the proposed mechanisms are lightweight; this should be quantified in terms of the introduced delay in the system. The results prove that the presented mechanisms increase the system flexibility whereas at the same time impose minimum performance overhead.

This paper is structured as follows. Existing research activities on adaptable protocols are presented in section 2. The introduced mechanisms enabling self-configuring protocols are briefly analysed in section 3, focusing on the end-to-end support signalling for the realisation of dynamic component binding and configuration. Section 4 proves the arguments for applicability, feasibility and performance evaluation through simulations using the UDP-based Data Transport (UDT) protocol [7]. Finally conclusion remarks and directions for future research are drawn in section 5.

2 Related Work

The ongoing proliferation of networking standards and the proved inefficiency of traditional protocol stack design have motivated numerous research efforts on the adaptation and customization of protocol layers or entire protocol stacks. Specifically, adaptable protocol stacks are seen as a technological enabler of next-generation networks which leverage the introduced adaptation and customization capacities to achieve two main goals: the dynamic adjustment of protocols' operation mode and the performance optimization of the operating protocols/protocol stacks. Such targets have been the main research objective of various adaptable protocol stack approaches, which are classified into the following three main categories - a detailed survey analysis on dynamically adaptable protocol stack frameworks is available in our previous work in [8].

- Adaptable protocols: This design approach introduces an extension protocol layer besides the generic part, for the implementation of custom protocol functions. It should be noted that this category employs a coarse granularity design since the fundamental design unit is a protocol layer or a set of them. Adaptable protocol stack frameworks include Conduits, JChannels and POEM [8]. For example, Conduit+ [9] proposes the specification of explicitly specified connections between Conduit+ objects under a generic object-oriented framework. The primary design goal of this framework is the reusability among software protocols.
- Composable protocols: this concept employs flat, hierarchical and graph-based models for building a customizable protocol/protocol stack out of fundamental protocol functions. Composable protocol stack frameworks include DiPS/CuPS , x-kernel, Coyote/Cactus, Appia, Ensemble, Horus, RBA, Da CaPo, ADAPTIVE, DRoPS, DIPS+, ACCORD and DPS [8]. For example, the Distributed Protocol Stacks (DPS) framework [10] enables the distribution of protocol functionality in network elements/nodes, targeting the optimization of the operations through functions migration.
- Reconfigurable protocols: This design allows for extending the traditional protocol stacks' composition schemes to support the dynamic binding and replacement of protocol components or even entire protocol layers during runtime, enabling service continuity and no loss of protocol data. Reconfigurable protocol stack frameworks include THINK, FRACTAL, GRPSFMT, DRAPS and Alonistioti [8]. In DRAPS, the fundamental unit is the core component which implements the protocol layer functionality and also realizes the communication with the adjacent protocol layers [11]. In addition, DRAPS facilitates dynamic protocol reconfiguration during runtime operation, also ensuring transparency. This is achieved by specifying the necessary interfaces per protocol component for the control of the reconfiguration operations (e.g. start/stop functions) and the state management procedures. We should point out though that this framework does not provide any details as regards the internal blueprints of the protocol stack architecture are not detailed.

At this point it should be noted that our approach falls under the category of reconfigurable protocols. The main advantage of our work is the detailed specification of a framework enabling the dynamic, semantic-based binding and replacement of protocol components during runtime operation of the protocol stack. In addition, the necessary support management functionalities and state management mechanisms were defined, targeting transparency, robustness and seamless operation.

3 Self-configuration Mechanisms

3.1 Background on Protocol Reconfiguration

The key concepts of protocol reconfiguration have been thoroughly investigated in our previous work in [6]. This section presents shortly our work on the protocol reconfiguration framework, which is based on the concept of protocol decomposition into components and their dynamic binding into specific protocol functionality. Specifically, this framework adopts a modular approach for both the protocol stack design and adaptation. The following design assumptions were made:

- A protocol stack is viewed as a composition of specific protocol layers,
- A protocol layer is viewed as a composition of protocol components.

Such modular protocol stack design affects both the protocol stack bootstrap and the protocol reconfiguration procedures. During protocol stack bootstrap, the dynamic component binding takes place to form both the protocol layer and protocol stack functionality. This is realized evaluating a semantic layer of information that accompanies each protocol component: its metadata. Specifically, two types of defined parameters are distinguished: a) protocol ID parameters; such parameters are related to the identification of the protocol, i.e. name, modularity, vendor, etc. b) protocol component parameters which include ID and binding parameters per protocol component and performance parameters per protocol layer. The protocol component binding parameters include component input and output interfaces information.

During protocol reconfiguration, the new configuration of the protocol stack is specified which includes the protocol layers that are used as well as the components that form these layers. Depending on the specified reconfiguration actions, one or more protocol layers may need to be replaced or one/more protocol components within each layer.

Semantic-Based Dynamic Binding of Protocol Components

The semantic-based dynamic binding of protocol components is realised evaluating the dynamic characteristics of the component's metadata and identifying their communicating counterparts - components. After the validation and verification of the composition, the communication links for the protocol components are established. This is realised by creating a FIFO queue per communication link for each component. The composition verification and establishment procedures are repeated for all the protocol components that are bound to the specified component.

Dynamic Replacement of Protocol Components

After evaluating the new protocol configuration, the replacement of the old protocol component with the new one is realised by a coordinating management entity, the Component Binding Control Module (CBCM). At first, the CBCM module pauses the functionality of the component under replacement and retrieves its execution state. Next, it instantiates the new component and dispatches to it the retrieved state information. Based on the acquired state information and its metadata, the new component realizes its dynamic composition with existing software components (by accessing the FIFO queues corresponding to existing communication links). The above analyzed on-the-fly replacement process also allows the reliable operation of the protocol under configuration, since it applies state management models to ensure the transparent switching from the old to the new component [6].

3.2 End-to-End Signalling Supporting Self-configuring Protocols

This section focuses on the realization of protocol reconfiguration in a system analyzing the required end-to-end supporting signalling (Fig. 1). In this work we consider the system model for dynamic adaptation of mobile devices in cognitive radio networks that is presented in our previous work [2]. Such system model encompasses the fundamental capabilities for the implementation of cognition in a system, namely monitoring the environmental stimuli, decision specification based on the contextual evaluation and realization of the adaptation through decision enforcement [12]. In such model two main physical entities are considered, namely the mobile devices and the network nodes. Based on the proposed capabilities, the following functionality is introduced in the mobile devices and network nodes:

- The Context Management (CTxM) module, which realises the administration of profile information (e.g. terminal and user profile, protocol stack stratifications).
- The Self-Configuration (Se-Co) module, which orchestrates the dynamic adaptation of the system protocol resources.
- The Autonomic Decision-Making module (ADM), which realizes the decision specification evaluating different options and alternatives. In this case study we consider that the decision is distributed between the network and the mobile device.

As regards the end-to-end supporting signalling, we assume that following a change in the environmental stimuli, a trigger for changing the device configuration takes place. Specifically, this could be the result of low QoS or low signal strength due to user mobility or could be caused by increased application requirements of a new service initiated by the user. In such cases, the ADM module located at the mobile device communicates with the CTxM module (also in the mobile device) to retrieve contextual information regarding the user and terminal profile and the protocol stack configurations (Fig. 1). After filtering this information and deciding the protocol stack requirements, ADM specifies a set of possible decision alternatives which are communicated to the network side ADM for evaluation. The latter should select the best one for the overall system optimality, taking into account various parameters including for example the network load, the a-posteriori operations that need to be implemented following the implementation of a specific alternative (e.g. handovers), load balancing schemes etc.

Upon receipt of the selected alternative, the ADM module at the mobile device communicates with the Se-Co module for the alternative implementation. In this scenario we consider that the selected option is the RAT upgrade which concerns the dynamic replacement of a protocol component in an operating protocol. Next, the Se-Co module implements all the necessary operations for this replacement. It communicates with the CBCM module which realizes the following operations: a) pauses the old protocol component, b) retrieves its state, c) instantiates and initializes the new component, and d) configures the state of the new component using state management schemes. The establishment and initialization of the communication links for the new component is also handled by the CBCM by evaluating semantic information for each component (section 3.1).

Following this description we identify that the concept of self-configuring protocols requires: a) message exchange between the mobile device and the network side for the evaluation and selection of the alternatives and decision-making functionality at the network side and b) self-configuration functionality and mechanisms in the mobile device for the dynamic component replacement. The first one may impose additional overhead at the network side – this case is investigated in detail in [2]. The second case concerns the overhead that may be imposed in the mobile device and is the focus of this paper.

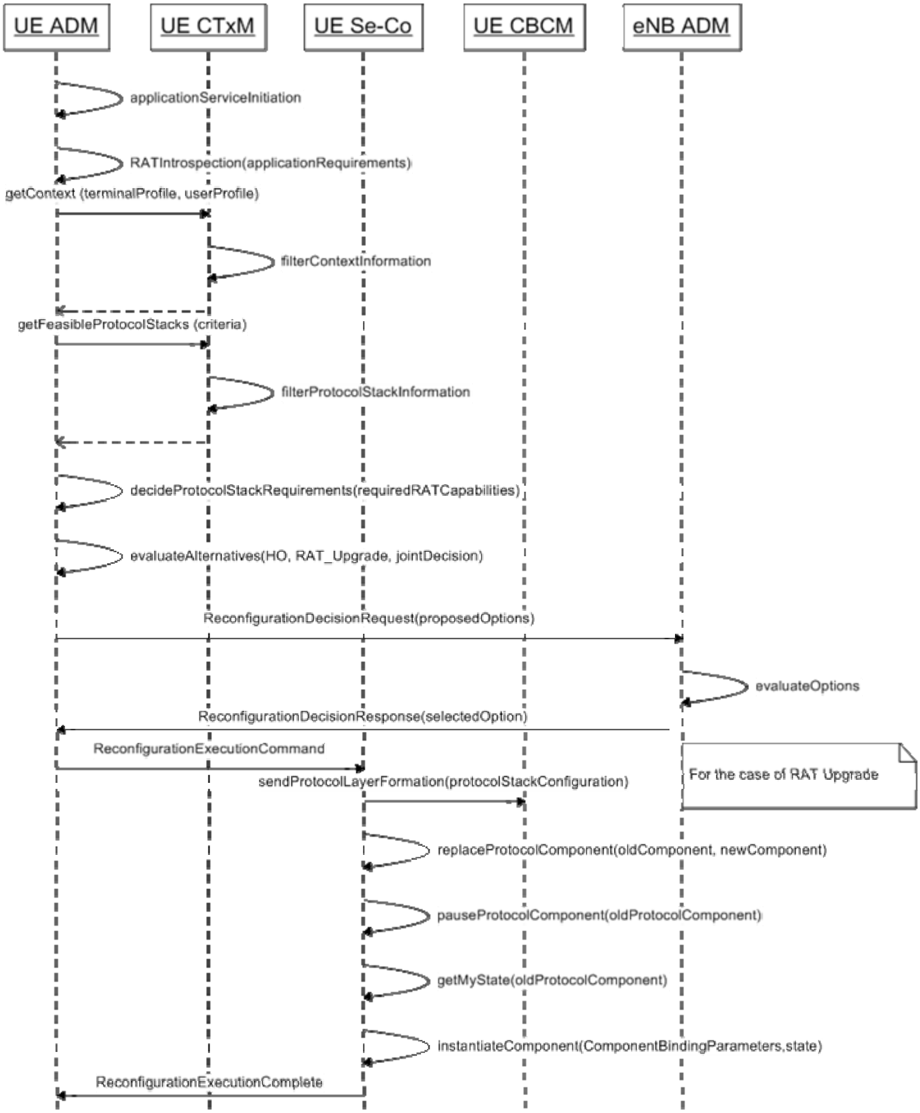

UE ADM
UE CTxM
UE Se-Co
UE CBCM
eNB ADM
applicationServiceInitiation
RATIntrospection(applicationRequirements)
getContext (terminalProfile, userProfile)
filterContextInformation
getFeasibleProtocolStacks (criteria)
filterProtocolStackInformation
decideProtocolStackRequirements(requiredRATCapabilities)
evaluateAlternatives(HO, RAT_Upgrade, jointDecision)
ReconfigurationDecisionRequest(proposedOptions)
evaluateOptions
ReconfigurationDecisionResponse(selectedOption)
ReconfigurationExecutionCommand
For the case of RAT Upgrade
sendProtocolLayerFormation(protocolStackConfiguration)
replaceProtocolComponent(oldComponent, newComponent)
pauseProtocolComponent(oldProtocolComponent)
getMyState(oldProtocolComponent)
instantiateComponent(ComponentBindingParameters,state)
ReconfigurationExecutionComplete

Fig. 1. End-to-end support signalling for protocol reconfiguration triggering and realization

4 Performance Evaluation

The introduction of dynamic reconfiguration capabilities in the protocol stack increases its flexibility but – inevitably – incurs a performance penalty [6]. Since one key issue in such a system is whether protocol reconfiguration forms an applicable and lightweight solution, the performance aspects should be investigated in the overall system operation. As regards the mobile device, the delay of the protocol reconfiguration procedure should be examined. Another objective concerns how the system operation is affected by the introduced delay and the protocol reconfiguration procedure, e.g. in terms of service continuity. Taking into account the component-based notion of the proposed solution, the component binding delay (the time required for the realisation of the binding operation) and component execution time (the time required for the execution of a specific algorithm/functionality that is incorporated in a component) are investigated using simulations.

4.1 Simulation Environment

The evaluation methodology used for the performance analysis of the self-configuring protocols solution is analysed herein. The performance analysis of the self-configuring protocols concept is evaluated through NS-2 simulations which target the component binding delay and the component execution time KPIs. In order to evaluate the key concepts of the self-configuring protocols solution, we selected to use the UDP-based Data Transport (UDT) protocol [7].

UDT is an application level data transport protocol for the emerging distributed data intensive applications over wide area high-speed networks (e.g., 1 Gb/s or above). UDT uses UDP to transfer bulk data and it has its own reliability control and congestion control mechanism. This new protocol is not only suitable for private or QoS-enabled links, but also for shared networks. UDT is also a composable framework that can accommodate various congestion control algorithms. Its reliability and congestion control mechanisms exist entirely in user space (not kernel space) and thus protocol variables are accessible at run time. However, UDT protocol configuration (congestion control algorithm selection) can only be done at compile time. In this layered architecture, the UDT layer is completely in user space above the network transport layer of UDP, whereas the UDT layer itself provides transport for applications. Meanwhile, applications provide optional control handlers to UDT as callbacks. In our work, the decomposition of the UDT protocol in 2 protocol components is modelled, considering a server node which implements UDT as a self-configuring protocol and a client node with a non-modular approach. A graphical representation of the component-based UDT protocol stack supporting protocol reconfiguration is provided in Fig. 2.

The simulations concern the evaluation of the communication control part of the two key protocol components, namely:

- the congestion control (CC) component which implements the congestion control functions,
- the UDT core component which implements the remaining functionality of the UDT protocol (i.e. connection establishment, memory and buffer management).

Both these components are implemented in two different agents and form the modular server node. The client node is implemented as a separate agent using a non-modular approach [13].

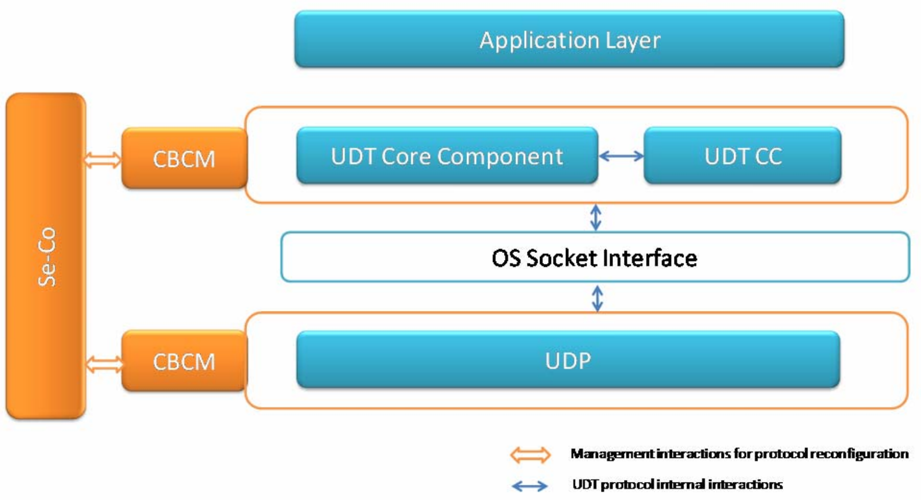

Application Layer
Se-Co
CBCM
UDT Core Component
UDT CC
OS Socket Interface
CBCM
UDP
Management interactions for protocol reconfiguration
UDT protocol internal interactions

Fig. 2. UDT component-based protocol stack supporting protocol reconfiguration

The deployment scenario is based on the binding of the core UDT component (hereafter referred as *Core*) with a congestion control algorithm (hereafter referred as *CC*) according to the afore-described methodology. Initially, the Component Binding Control Module retrieves the components metadata. Then the composition of the two components is checked and the required structures are created. In this scenario, we also consider the dynamic replacement of the CC component implementing CVegas [14] with another CC component implementing CTCP [15]. CVegas is a delay-based algorithm that uses its own data structure to record packet departure timestamps and ACK arrival timestamps and then calculates accurate RTT values. CTCP is an application level implementation of the standard TCP algorithm using the UDT/CCC library [15]. In addition, it is assumed that the Core Component is bound to the same components as the CC component. At first, the Component Binding Control Module retrieves the metadata for the new component (CC with CTCP) and checks which components it is composed with. Then it pauses the function of the component to be replaced (CC with CVegas). Thereafter, the Component Binding Control Module retrieves the state of CC-CVegas component and sets the state of CC-CTCP to the same state. This is necessary since the replacement of a component, which is in a specific state, with a component that is in an idle or initial state, does not guarantee the reliable operation of the protocol [13]. It should be noted that besides CVegas, various algorithms for the congestion control component have been considered in the simulations.

4.2 Results

This section presents the results derived from the NS-2 simulations of the self-configuring protocols. In order to better compare the results, the minimum, maximum and mean value of the component binding delay and the component execution time are computed per algorithm implementing the congestion control component. The results are presented in Fig. 3 and Fig. 4. Such figures were obtained considering the following algorithms for the implementation of the CC component: TCP, Scalable TCP, High-Speed TCP, Binary Increase TCP, TCP Westwood, TCP Vegas and Fast TCP. Scalable TCP is a simple sender-side alteration to the TCP congestion window update algorithm which offers improved performance in high-speed wide area networks [16]. HighSpeed TCP is a modification to TCP's congestion control mechanism for use with TCP connections with large congestion windows [17]. Binary Increase TCP offers an optimized congestion control algorithm for high speed networks with high latency enabling the algorithm to aggressively increase its transmission speed toward the maximum allowed by the high-speed network [18]. TCP Westwood is a sender-side-only modification to TCP NewReno algorithm and it aims to better handle large bandwidth-delay product paths, with potential packet loss due to transmission or other errors, and with dynamic load [19]. Fast TCP is a TCP variation that measures a different factor (queuing delay instead of loss probability) to evaluate network congestion and can increases its congestion window more quickly than TCP [20].

As regards the component binding delay, the maximum value equals 337 μsec and it is obtained for the TCP Westwood algorithm, whereas the minimum value is obtained for the UDT algorithm and equals 72 μsec. In addition, as regards the component execution time, the maximum value equals 193 μsec and it is obtained for the Fast TCP algorithm, whereas the minimum value is obtained for the scalable TCP, Binary Increase TCP, TCP Westwood and UDT algorithms and equals 32 μsec.

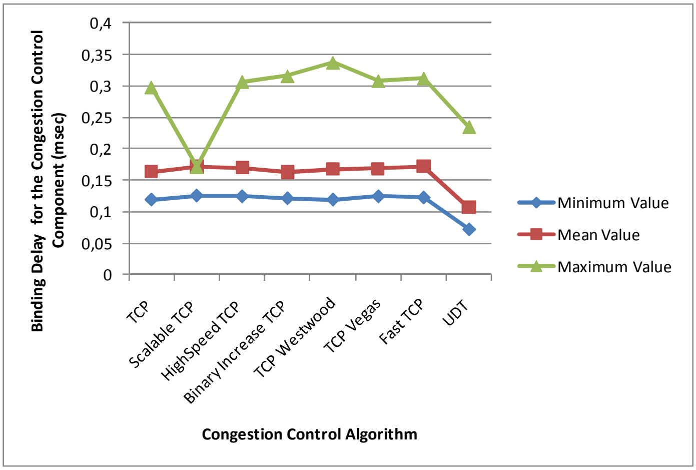


Fig. 3. Minimum, maximum and mean values of the binding delay for the congestion control component based on simulation results for different algorithms

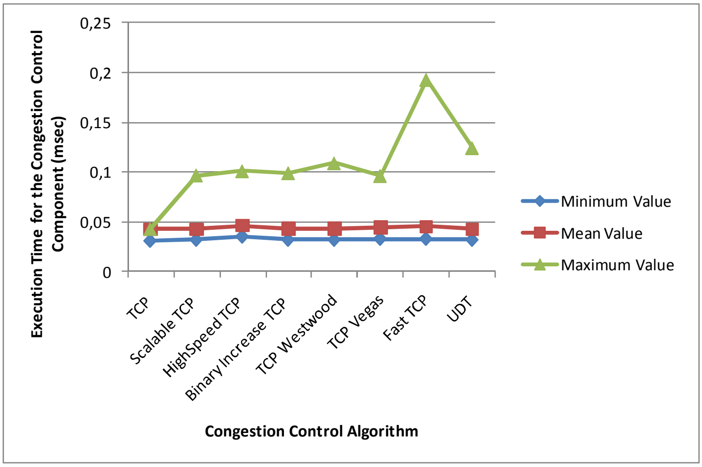


Fig. 4. Minimum, Maximum and Mean values of the Execution Time for the Congestion Control Component based on Simulation Results for Different Algorithms

The simulation results have proven the feasibility of the self-configuring protocols solutions. More specifically, the simulation results proved that the UDT protocol components are successfully bound together forming the full functionality of the UDT protocol. The correctness of the presented framework was also confirmed by the successful execution of the congestion control operations. It should be noted that the induced component binding and component execution delays were very low for all the tested congestion control algorithms and did not affect the overall system operation [13]. In addition, the simulation results have proven that the dynamic binding and execution of different types of functionalities/algorithms does not affect the performance of the reconfiguration procedures. This fact validates the feasibility and applicability of employed framework and mechanisms in a component-independent manner.

It should be noted that the evaluation of the concept through experiments in proof-of-concept prototype platforms has been also realised [13]. Such results complement the simulation analysis and have also proven the applicability of the protocol modularisation and self-configuration operations during real system operation. In addition, it should be noted that the presented framework does not affect the system functions (the applications runs smoothly despite the changes) - however the results in the RTT delay are significant. Based on real time measurements acquired during demonstrations, the RTT delay with CTCP is reduced to 1/3 of the RTT delay with CVegas.

5 Conclusions

This paper discusses the introduction of enhanced autonomous functionalities in mobile terminals to enable their intelligent protocol auto-configuration. Specifically, the basic system model for the support of such functionality and respective end-to-end signalling has been proposed. The operational stages required for protocol reconfiguration have been analyzed, discussed, and assessed through simulation results.

The results proved that the mechanisms for component-based protocol are lightweight, yielding a feasible approach. Such approach introduces negligible delay to the system, but it does not affect the viability of the system's operation.

Acknowledgements

This work was funded by the European Commission Seventh Framework Programme ICT-2008-224344 through the Self-NET Project (https://www.ict-selfnet.eu). The authors would like to thank their partners in the IST SELF-NET project for insightful technical discussions that triggered the development for the material presented herein.

References

1. Dobson, S., Denazis, S., Fernández, A., Gaïti, D., Gelenbe, E., Massacci, F., Nixon, P., Saffre, F., Schmidt, N., Zambonelli, F.: A survey of autonomic communications. ACM Trans. Auton. Adapt. Syst. 1(2), 223–259 (2006)
2. Patouni, E., Alonistioti, N., Merakos, L.: Cognitive Decision Making for Reconfiguration in Heterogeneous Radio Network Environments. IEEE Transactions on Vehicular Technology (TVT), special issue on Achievements and the Road Ahead: The First Decade of Cognitive Radio, PP(99) (2010)
3. Mahmoud, Q.: Cognitive Networks: Towards Self-Aware Networks. Wiley, Chichester (2007) ISBN: 978-0-470-06196-1
4. Miller, J., Thomson, P.: Beyond the complexity ceiling: evolution, emergence and regeneration. In: Proc. GECCO 2004 Workshop on Regeneration and Learning in Developmental Systems (2004)
5. Bouabene, G., Jelger, C., Tschudin, C., Schmid, S., Keller, A., May, M.: The autonomic network architecture (ANA). IEEE Journal on Selected Areas in Communications 28(1), 4–14 (2010)
6. Alonistioti, N., Patouni, E., Gazis, V.: Generic architecture and mechanisms for protocol reconfiguration. Special Issue on Reconfigurable Radio Technologies in Support of Ubiquitous Seamless Computing, Mob. Netw. Appl Journal 11(6), 917–934 (2006)
7. Gu, Y., Grossman, R.L.: UDT: UDP-based Data Transfer for High-Speed Wide Area Networks, Computer Networks. The International Journal of Computer and Telecommunications Networking 51(7), 1777–1799 (2007)
8. Gazis, V., Patouni, E., Alonistioti, N., Merakos, L.: A Survey of Dynamically Adaptable Protocol Stacks. IEEE Communications Surveys and Tutorials 10(1), 3–23 (2010)
9. Sahlin, B.: A conduits+ and java implementation of internet protocol security and internet protocol, version 6, Master's thesis (1997), `http://citeseer.ist.psu.edu/286786.html`
10. Kliazovich, D., Granelli, F.: Distributed protocol stacks: A framework for balancing interoperability and optimization. In: IEEE International Conference on Communications Workshops 2008 (ICC Workshops 2008), pp. 241–245 (2008)
11. Niamanesh, M., Jalili, R.: A dynamic-reconfigurable architecture for protocol stacks of networked systems. In: Proceedings of the 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), Washington, DC, USA, vol. 1, pp. 609–612 (2007)

12. Mitola III, J.: Cognitive Radio for Flexible Mobile Multimedia Communications. Mob. Netw. Appl Journal 6(5), 435–441 (2001)
13. Patouni, E., Holland, O., Alonistioti, N.: Cognitive Functionalities for Mobile Terminal Self-Recovery and Protocol Auto-Configuration. In: The Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications 2008 (PIMRC 2008), Cannes, France (2008)
14. Brakmo, L., Malley, S.O., Peterson, L.: TCP Vegas: New techniques for congestion detection and avoidance. In: Proceedings of the SIGCOMM 1994 Symposium, pp. 24–35 (1994)
15. Tan, K., Song, J., Zhang, Q., Sridharan, M.: A Compound TCP Approach for High-speed and Long Distance Networks, Technical Report MSR-TR-2005-86, Microsoft Research (2005)
16. Kelly, T.: Scalable TCP: improving performance in highspeed wide area networks. ACM SIGCOMM Computer Communication Review 33(2) (2003)
17. Floyd, S.: HighSpeed TCP for Large Congestion Windows, RFC 3649, Experimental Standard (2003)
18. Xu, L., Harfoush, K., Rhee, I.: Binary Increase Congestion Control for Fast Long-Distance Networks. In: Proceedings of IEEE Infocom 2004, Hongkong, China (2004)
19. `http://www.cs.ucla.edu/NRL/hpi/tcpw/`
20. Jin, C., Wei, D.X., Low, S.H.: FAST TCP: motivation, architecture, algorithms, performance. In: Proceedings of IEEE Infocom 2004, Hongkong, China (2004)

Analysis of the Energy Consumption of JavaScript Based Mobile Web Applications

Antti P. Miettinen[1] and Jukka K. Nurminen[1,2]

[1] Nokia Research Center, Helsinki, Finland
`{antti.p.miettinen,jukka.k.nurminen}@nokia.com`
[2] Aalto University School of Science and Technology, Finland

Abstract. JavaScript is the dominant language of modern web applications. In this research, we have investigated the battery-consumption of JavaScript applications running on mobile phones. In our empirical study, we developed and analysed eight implementations of the same application using different JavaScript libraries. The results show that there are significant differences between different implementations. There is no single factor explaining the performance differences. Furthermore, the performance of different libraries is strongly affected by the communication technology (3G or WLAN). The long latencies that 3G introduces suggest that increasing the parallel execution of server queries has potential for energy and speed improvements.

Keywords: Energy-efficiency, mobile services, JavaScript, web-applications.

1 Introduction

Recently the emphasis of software development has shifted from applications to services. Instead of installing specific software, the end user devices access services residing on the Internet servers. The shift that started on the PC side is gradually also happening with mobile phones and can extend to other lightweight wireless devices.

In many respects the mobile devices, such as modern smart phones, resemble PC devices. They are more limited in resources but the difference is not very big: modern smart phone has roughly the same CPU power, amount of RAM memory, and file storage capacity as PC computers less than ten years ago. However, a fundamental difference between PC computers and mobile devices is sensitivity to energy consumption. Because a mobile device has only intermittent access to electricity grid, it is essential that it is able to run hours, preferably days, without recharging. The progress on battery technology is slow; the annual growth of battery capacity is around 5% [1]. This is much less than the rapid growth of CPU power, memory capacity, and communication bandwidth. Therefore, energy-efficiency is of primary concern for the design of wireless devices and applications, and is likely to remain so also in the future.

JavaScript is an important building block for modern web applications and a key component of the AJAX paradigm [2], which enables the development of interactive and dynamic web services. Initially, JavaScript was developed to add dynamic effects to web pages with small code snippets. Since JavaScript was originally not intended for large-scale programming, its use to implement complex web applications of today

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 124–135, 2010.
© Springer-Verlag Berlin Heidelberg 2010

is not trivial for the developers. The developers work is further complicated by the fact that different browsers require slightly different JavaScript code sequences for the same tasks.

One way to make JavaScript programming easier is to use JavaScript libraries which package widely used functionality into reusable modules and, at the same time, isolate the developer from the differences of the underlying platforms. As there are a number of libraries available, it is not easy for the developer to choose which one is most applicable for each task. The problem is even more difficult for the mobile web service developer since there is hardly any information about how the different libraries work on mobile devices.

In this research, we investigate the JavaScript libraries and their use on mobile devices. In particular, we focus on the energy consumption of different libraries. Does the JavaScript library selection influence the energy consumption of the mobile web service? Which libraries enable energy-efficient application development? What are the essential reasons for the differences?

These issues have immediate importance for current mobile phones and applications targeted for them. However, similar issues are likely to be important also for other lightweight wireless devices, many of which could be even more sensitive to battery consumption.

It would be nice if the same languages and tools could be used to develop applications for highly heterogeneous devices. This would save the training costs of the developers, reduce the need of different implementations for different devices, and allow the progress made on web development to be applied to a variety of devices in a short time span. Finding out if this is possible and, especially, if battery consumption is a problem is one of the contributions of this research.

Although the battery consumption is often mentioned as a problem for mobile AJAX applications [3-5], there has been little prior research on JavaScript energy-efficiency. To our knowledge, our research is the first one to analyze systematically the energy-consumption of an AJAX application.

The rest of the paper is structured as follows. Section 2 reviews related research. Section 3 describes our empirical experiment where eight developers implemented the same web application using different libraries. Section 4 presents the measurement results of the performance of these applications. Section 5 discusses and analyses the results. Finally, section 6 concludes the paper and presents ideas for further research.

2 Related Research

Hansen [6] and Walton [7] have investigated the browser power consumption on PC hardware. Hansen's work is more driven by the "green thinking" that is how much electricity is needed to run web applications. On mobile computing, this approach is also relevant but of lesser importance than the inconvenience that frequent recharging causes to the user. Hansen looked at the effect of different elements of a web page to energy consumption. His finding was that Flash banner ad was the most harmful for energy consumption but all client side scripting technologies, JavaScript, Java, VBScript and Silverlight, tend to increase the energy consumption. Walton compares different browsers on three different processors. His results show that there are no major differences in energy consumption between popular browsers (with the exception of Safari 4, which is consistently worse than others on all platforms).

Wei [8] has investigated the performance of JavaScript in different browsers on PC environment. His results show that different browsers have different performance bottlenecks although there are some common problems.

Other studies focus on JavaScript execution performance without explicit analysis on energy consumption. Sounder [9] has investigated the JavaScript more from the developer perspective. He comes up with a set of rules that make JavaScript more effective (Frontend performance best practices). Kiciman and Livshits [10] have analyzed JavaScript behavior and developed an end-user tool to give visibility to a web applications performance.

Pervilä's research [5] is one the few studies that explore the use of AJAX applications on mobile devices. The analysis is mainly focused on how the AJAX application work on mobile environment as well as on the execution speeds. He notes the relevance of battery consumption and analyzes it briefly. He does not measure energy on a detail level but uses the frequency of battery recharging as the unit for energy consumption.

Some studies compare different ways to implement the same web application functionality. Smullen and Smullen [11] compare two implementations of a university student information system; one based on HTML and one based on AJAX. AJAX provides significant performance improvements (40-70%) but only when appropriate caching is in use. In a worst-case scenario it performed worse (10-15%) than the traditional HTML application. Xie and Parsons [12] compare the use of an AJAX application and an Active Server Pages (ASP) application with identical functionality in GPRS networks. There results are mobile Ajax over GPRS can reduce the bandwidth requirement by about 70% and cut the server's response time in half.

3 Research Methodology

In order to understand how the performance of JavaScript libraries influences the battery consumption of a web application we implemented the same task with different libraries. Different implementations were done by computer science students at Aalto University who were either at the final year of their master studies or at post-graduate level. The test group thus presented technically skilled developers who had experience in programming with various languages. However, most of the persons did not have prior experience with JavaScript development.

3.1 Task Specification

The students were first taught how to develop web applications and write JavaScript code. Then they were given the following task.

Develop an application that allows a person to see if friends are nearby. Your application should have the following display. Center person, Location, and Distance are editable fields. Distance to friends should be populated by those friends who are within the specified distance from the Center person.

Center person: Peter
Location 12345 6789
Distance: 5 km

Distance to friends
John 3 km
Paul 4 km
Mary 5 km

The application should support three tasks

1. *Select the center person from a listbox*
2. *Change the distance*
3. *Change the location of friend (with another browser) to see that the friend list is able to detect the change and update itself. Note that this step requires advanced AJAX concept "long poll".*

When the above changes are made, the rest of the page should be updated automatically using the AJAX techniques.

Each student was free to choose the JavaScript library to suit his taste. The following libraries were used:

- MooTools http://mootools.net/
- Dojo http://www.dojotoolkit.org/
- ExtCore http://www.extjs.com/products/extcore/
- Prototype http://www.prototypejs.org/
- YUI (two implementations) http://developer.yahoo.com/yui/
- jQuery http://jquery.com/
- GWT http://code.google.com/webtoolkit/

Note that GWT, Google Web Toolkit, differs from the other libraries in the respect than instead of writing JavaScript code and calling the library functions from the code, the GWT developer writes Java code, which the system compiles into JavaScript.

The same server side implementation hosted at a university server was used by all applications. The server side was based on Apache and python code and was used via a REST interface (http://maps.cs.hut.fi/cloud/index.php/Server_API).

3.2 Measurement Setup

For the measurements, we used Nokia N900 mobile phone with the built-in browser. The measurements were done with Nokia Energy Profiler, which is a software-only analysis tool for Nokia mobile phones available at Forum Nokia (www.forum.nokia.com). In addition to power consumption, it is able to measure downlink and uplink bitrates, CPU load, memory usage, and some other attributes.

In our measurements, we performed the following steps:

- Initial page load (no center person specified)
- Select a person e.g. Peter
- Change distance from 5 (default) to 2
- Move John from x to y with another browser

For each step we used the Nokia Energy Profiler to record the execution time, CPU load, average power consumption, and the number of bytes uploaded and downloaded.

We used Elisa cellular operator for the 3G measurements. The measurements were done in residential suburban area, where HSDPA (3.5G) functionality was available. For WLAN measurements, we used a 802.11g access point, which was connected to the public Internet via ADSL.

We repeated each measurement five times to compensate the inherent performance variability of live networks that arise e.g. from varying signal quality, activities of other users, and other similar external causes that are beyond our control.

4 Results

Figure 1 shows the cumulative energy consumption, amount of downloaded and uploaded data, CPU usage, and execution time for the complete use case. To get these values we measured each step separately five times and summed up the averages of each step. Note that if in a real case the steps were executed tightly one after another the results might differ a bit from our measurements because the “hot start” for the later steps could influence the results. The data in Figure 1a is from the case when the mobile phone was using 3G and the data in figure 1b is from using wireless LAN (802.11g) and ADSL to communicate with the server. The unit on the y-axis presents the energy (Joules) while the heights of the bars that represent other attributes are relative values that allow comparisons between different libraries and carrier technologies.

It is clearly visible from Figure 1 that there are differences between different libraries. Cumulative energy, amount of data, CPU usage, and execution time vary considerably from one implementation to the other. As expected WLAN was clearly more energy efficient and had a faster execution time than 3G. However, the other dependencies are more complicated. There is no clear correlation between energy and execution time, energy and amount of data, or energy and CPU usage. It seems that the energy consumption is dependent on these attributes in a non-trivial fashion.

Some observations are easy to derive. First, for GWT the additional complexity arising from the automatically generated JavaScript code clearly increases the amount of data transferred. However, the larger amount of data does not directly translate into increased energy consumption. GWT is one of the most energy hungry implementations but the difference in the amount of transferred data is far bigger than the difference in energy consumption in comparison with the other implementations.

Figure 2 shows the energy consumption for each step of the test case. It can be seen that there is a lot of variability in the charts. For MooTools the intial step was dominant in 3G while in WLAN it is on par with most of the libraries. This cannot be explained only by large data size because in Prototype much more data transfer is happening.

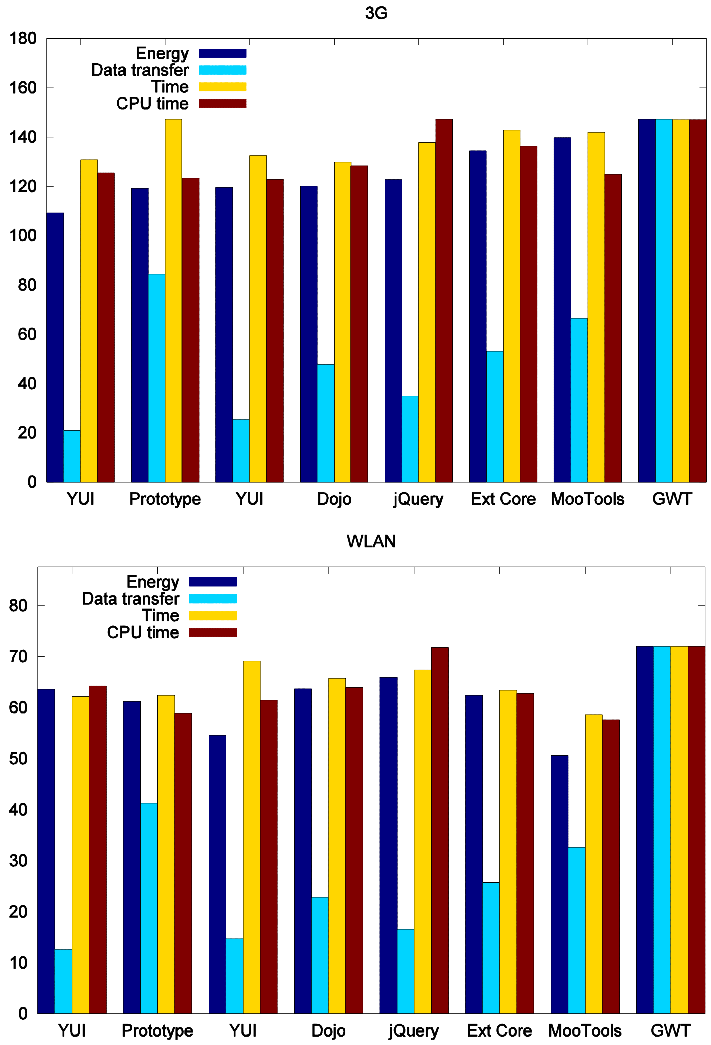


Fig. 1. The cumulative energy consumption, amount of downloaded and uploaded data, CPU usage, and execution time for the complete use with a) 3G and b) WLAN

The relative energy consumption of different steps seems to vary between the libraries. For many libraries, the differences are so small that they can be attributed to measurement error.

With 3G for many libraries the “Change distance” step was the dominant energy consumer while with WLAN the role of “Move friend” and “Select” are with many libraries the most significant ones.

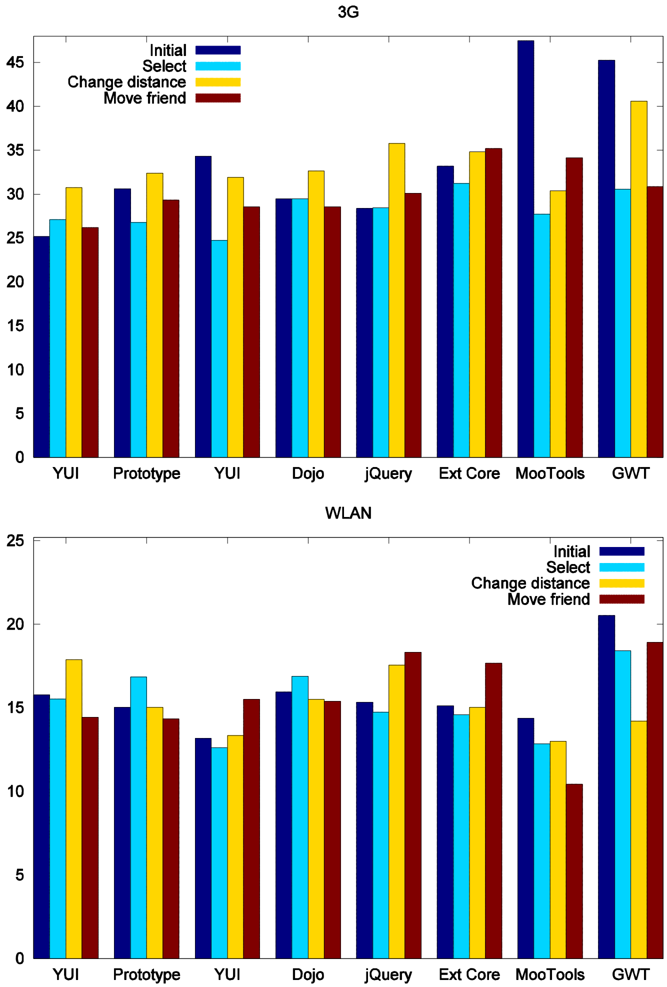


Fig. 2. Energy consumption split to the different tasks with a) 3G and b) WLAN

To understand the reasons for the performance differences we plotted the data transfer as a function of execution time in Figure 3. This example analyzes the MooTools implementation but the behavior of the other implementations is similar with minor variations. The dotted (green) curves show the downlink bitrate (in kilobytes per second) while the solid (red) curve shows the same for the uplink.

An obvious difference is the higher bitrate that WLAN is able to reach, which is about double the 3G data transfer. However, since the amount of data to be transferred is quite small, there is no significant difference in the execution time of the active data transfer. However, the long latency of 3G is a far more important component. The arrow in Figure 3 a) shows the time when the first GET request is issued. After that, it takes almost two seconds before the download starts. In WLAN case Figure 3 c) the download starts almost immediately after the GET request has been issued.

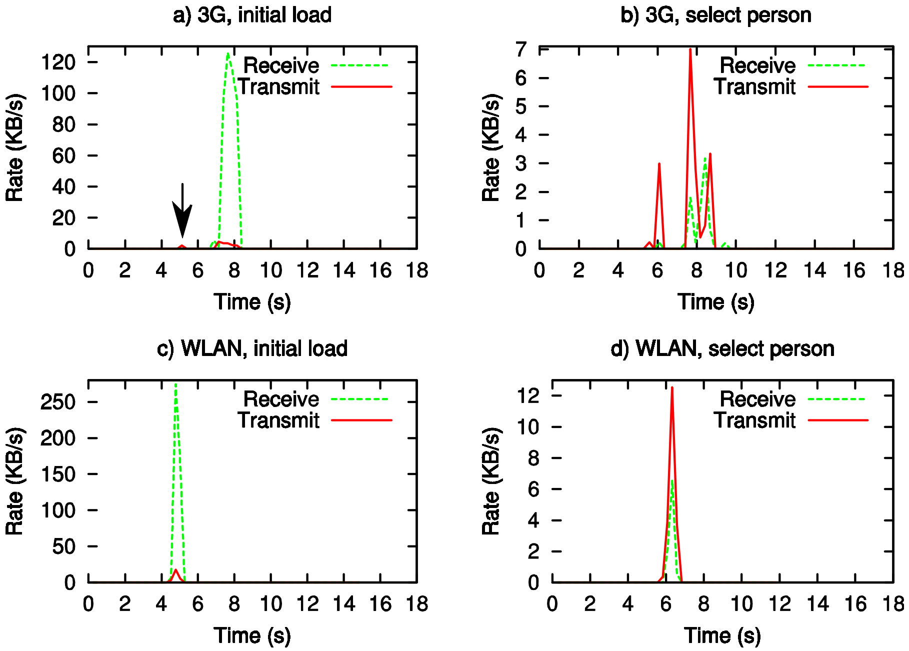


Fig. 3. MooTools data transfer charts for the first two steps, initial load (a&c) and select person (b&d)

This effect of latency becomes even clearer when the use case is more complicated. The "Select person" task plotted in Figure 3 b) and d) consists of five GET requests. These requests are executed in three phases so that the execution does not progress before each GET request of a phase has been completed and the server has returned their results. Because of the long latency, these requests are clearly separate in Figure 3 b) while in the WLAN case (Figure 3 d) they seem to merge to a single data transfer. The key lesson from this is that the more parallel execution of http requests the code has, the better the performance especially with high latency networks like 3G.

To analyze the sensitivity of our results, we performed measurements with an additional device, the Nokia E71 phone. Our primary test device Nokia N900 is a high-performance multimedia oriented mobile computer with a touch display while E71 is a traditional smart phone with a smaller display and more limited resources. Another difference between N900 and E71 is that the former is based on the Maemo Linux operating system while the latter uses Symbian. Figure 4 plots the correlation of the execution time and energy consumption with WLAN communication. It shows the measurements (averages ± error margins) with the two devices. The red measurements are with Nokia N900 and the green measurements are with Nokia E71. It is clear from the figure that there is strong dependency between execution time and energy spending.

This dependency is the clearest explaining factor for most of the energy differences in this study. During the execution, energy is spent on different hardware modules of the mobile phone. For instance, if the display is on during the execution then a

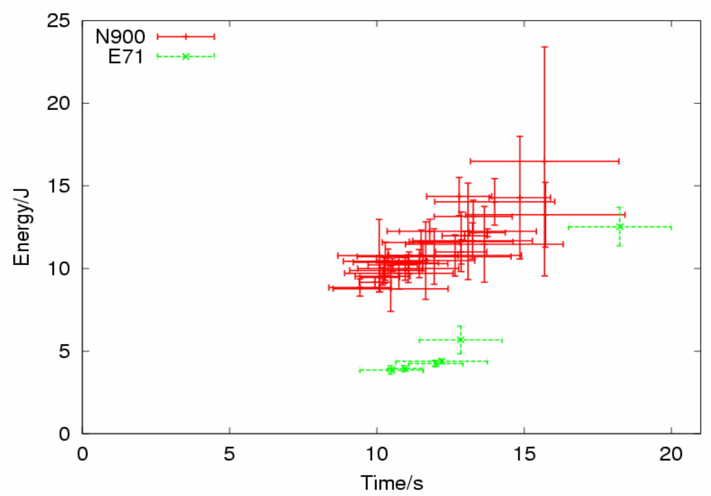


Fig. 4. Correlation between execution time and energy consumption

device with a larger display (N900) consumes more energy than a device with a smaller display. Memory and CPU are other components that are constantly drawing power during the execution.

5 Discussion

The results indicate that the library selection is relevant for web application energy-efficiency. With 3G, the difference between the most power hungry (GWT) and the least power hungry implementations was around 20%. With WLAN, the difference was 30%. Interestingly the least power hungry implementation was different for 3G and WLAN; with 3G it was YUI and with WLAN MooTools.

However, the energy difference is small in comparison to the difference in the amount of transferred data. The biggest implementation (GWT) required about five times more data transfer than the most compact one (YUI).

Although YUI was both the most compact and most energy-efficient implementation for 3G, it is wrong to draw the conclusion that the energy consumption differences can be explained by the transferred amounts of data alone. E.g. the data transferred by jQuery was about half in comparison to Prototype while the energy consumptions of the two implementations were about the same.

GWT is a special case compared to other libraries. While with other libraries the developers write JavaScript code, a GWT application is developed with Java and the JavaScript code used by the application is the result of a compilation process. The generality of this approach seems to result into large JavaScript code size. Especially in case of 3G the larger amount of data transfer is also reflected in energy consumption.

Execution time seems to be the attribute that best explains the differences in energy consumption between different implementations. Execution speed is not only good for energy consumption but also for user experience in the form of better response time.

However, the results do not rule out the effect of other factors although their influence is smaller. The simple conclusion is to use libraries with fast execution speeds. The good news is that the library developer when optimizing the speed of a library is at the same time optimizing the energy-efficiency as well.

Long latency is a major factor differentiating 3G from WLAN cases. Therefore finding ways to live with the long latency would benefit both the execution time and the energy consumption. The developers should be familiar with the issue and consider how to maximize the parallelism of server requests when developing web applications. However, it can be hard to realize because the typical development environment for mobile web applications is a PC, which normally has a high-speed, low-latency connectivity. Therefore, the issue only becomes visible when the web application is tested on a mobile device. A simple alternative is that development tools would allow the developers to experiement how their applications work when the latency increases. Another alternative would be to build automatic support for maximal parallel execution into the library or middleware code. The system would need to buffer the separate GET or POST requests and send them as a single entity to the server. Similar mechanism could also be useful at the server side. However, implementing such a mechanism could be difficult because detecting the dependencies between GET and POST calls automatically can be complicated.

When drawing conclusions based on this study it is important to keep in mind two limitations of our approach. First, it is impossible to filter out the individual differences in development style between different developers. However, as the task was relatively simple, there are no major algorithmic differences between the different implementations. Moreover, the two implementations with the YUI library have very similar performance, which gives some limited evidence that the differences between developers do not have major effect on the result.

Secondly, the application is very simple compared to many AJAX applications in use today. Do the results of this small-scale study scale when the application size increases? It is difficult to give a definite answer to this question. Typically, the larger applications consist of smaller modules. If the results of this study apply to a typical module then it is to be expected that they also apply for aggregates of such modules.

A further observation of this study is that all of the libraries work on mobile devices. This indicates that the mobile browsers have matured and that the resources of mobile devices are adequate for relatively complex tasks. It is important to note that none of the tested libraries has been targeted for mobile devices. In this respect, the difference between mobile handheld devices and PC computers is getting blurrier. However, the number of library functions needed for the test application is quite limited so it can be that for applications that are more complicated some of the libraries would experience problems.

Although the functional capability of the browsers on mobile devices is almost equal to browsers running on PC environment, important differences still exist. The usability of the application with a small display without mouse still needs improvement. Data transfer and rendering speeds could be further enhanced to make the response times faster. However, in this research we did not focus on these aspects as our target was to understand what the web application developer can do to create efficient applications.

6 Conclusions

The energy-efficiency of JavaScript based web applications is important for mobile phones and other lightweight devices. Battery-consumption is not only a device or hardware R&D topic but it can be influenced by application developers. In particular, in this research we have investigated how the web application developer can influence the battery consumption of the target devices of his application.

Although battery consumption is important for applications for mobile phones and other lightweight devices, the amount of prior research on the area is limited. In particular, as far as we are able to find out, this is the first empirical study about how JavaScript developer can influence the battery consumption of the target device.

Our research shows that there are relevant differences between different ways to implement JavaScript based application from the energy-efficiency point of view. By choosing a proper library, the user is able to save up to 30% of energy in the implementation of the same functionality.

In this experimental study, we have compared eight implementations of the same task with different JavaScript libraries. We have shown that the size of the code alone does not explain the difference in energy consumption. However, further research would be useful to verify and to extend our results via more controlled experiements. Moreover, better understanding of the reasons for the performance differences could be used to develop new libraries that would also consider the energy-efficiency dimension.

Experimentation with larger scale solutions would also be useful. Naturally, the bigger the software size the harder it is to create multiple implementation for comparison purposes. Moreover, in case of more complicated software the differences between design decisions that different developers make become more dominant making the comparison harder.

Acknowledgements. We are grateful to the participants of the Seminar on Distributed Systems at Aalto University in fall 2009 for the implementation of the test applications.

References

1. Robinson, S.: Cellphone Energy Gap: Desperately Seeking Solutions. Strategy Analytics (2009)
2. Garrett, J.: Ajax: A New Approach to Web Applications (2005), `http://www.adaptivepath.com/publications/essays/archives/000385.php`
3. Kunito, G.: Issues for mobile Ajax for cellular users (2007), `http://www.w3.org/2007/06/mobile-ajax/papers/docom`
4. Van De Walle, D., Goeminne, N., Gielen, F., Van De Walle, R.: Challenges for Mobile Gaming based on AJAX (2007), `http://www.w3.org/2007/06/mobile-ajax/papers/mobix`
5. Pervilä, M.: Performance of AJAX applications on mobile devices. MSc thesis, University of Helsinki (2008)

6. Hansen, R.: Browser Power Consumptions (2008), `http://www.sectheory.com/browser-power-consumption.htm`
7. Walton, J.: Browser Face-Off: Battery Life Explored (2009), `http://anandtech.com/mobile/showdoc.aspx?i=3636`
8. Wei, C.: A Study of Ajax Performance Issues (2008), `http://www.coachwei.com/blog/_archives/2008/1/22/3480119.html`
9. Souders, S.: High-performance web sites. ACM Commun. 51(12), 36–41 (2008)
10. Kiciman, E., Livshits, B.: AjaxScope: a platform for remotely monitoring the client-side behavior of web 2.0 applications. SIGOPS Oper. Syst. Rev. 41(6), 17–30 (2007)
11. Smullen III, C.W., Smullen, S.A.: Modeling AJAX Application Performance. In: 2nd IASTED International Conference on Web Technologies, Applications, and Services (2006)
12. Xie, F., Parsons, D.: Measuring Ajax Performance on a GPRS Mobile Platform (2008), `http://www.massey.ac.nz/~dpparson/Xie_Parsons_APIS7.pdf`

Equal Gain MIMO Beamforming in the RF Domain for OFDM-WLAN Systems

Álvaro Gonzalo[1], Ignacio Santamaría[1], Javier Vía[1],
Fouad Gholam[1], and Ralf Eickhoff[2]

[1] University of Cantabria, 39005 Santander, Spain
[2] Dresden University of Technology, 01062 Dresden, Germany

Abstract. Equal gain beamforming (EGB) schemes are typically applied in the baseband domain and hence require complex RF transceivers. In order to simplify the circuitry and energy consumption of the MIMO transceiver, in this paper we consider an EGB scheme that operates in the RF domain by means of analog phase shifters. Under OFDM transmissions, the design of the optimal phases is a complicated nonconvex problem with no closed-form solution. Building upon a previously proposed solution for flat-fading MIMO channels, this paper describes an alternating minimization algorithm to find an approximate (suboptimal) solution for the OFDM case. Monte-Carlo simulations are performed in order to demonstrate the effectiveness of this new analog beamforming scheme under coded and uncoded WLAN 802.11a transmissions.

Keywords: Analog Combining, Multiple-Input Multiple-Output (MIMO), Equal-Gain MIMO Beamforming, Orthogonal Frequency Division Multiplexing (OFDM), Wireless Local Area Networks (WLAN).

1 Introduction

Conventional multiple-input multiple-output (MIMO) systems require all antenna paths to be independently acquired and jointly processed at baseband. The hardware cost, complexity and power consumption are therefore increased accordingly. These drawbacks might explain, at least partially, why MIMO technologies have not found yet widespread use in low-cost wireless terminals. One way to increase the energy-efficiency of MIMO terminals and reduce their costs is to simplify the associated hardware and radio-frequency (RF) circuitry as much as possible, while still retaining some of the benefits provided by the MIMO channel (e.g., spatial diversity) by means of specifically designed signal processing algorithms. With this goal in mind, a RF-MIMO architecture that performs spatial processing directly in the analog domain is currently being developed within the EU-funded project MIMAX [1,2].

The combining scheme considered in [1,2], which is depicted for convenience in Fig. 1, permits to change the amplitudes and phases of the transmitted/received RF signals by means of vector modulators (VM). Therefore, for flat-fading MIMO channels and assuming perfect channel state information at both sides

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 136–147, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

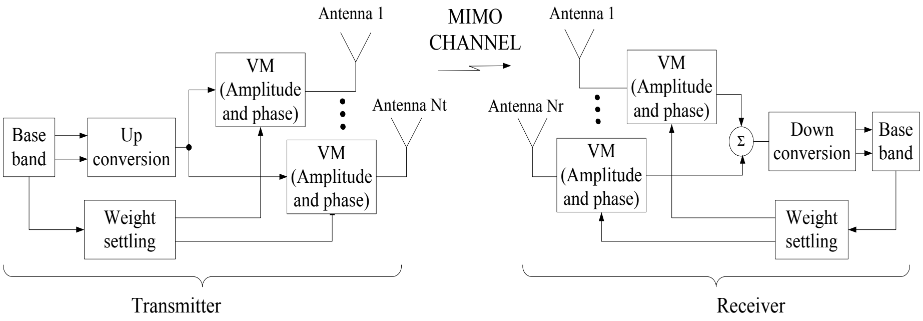


Fig. 1. Maximum ratio beamforming in the radio-frequency domain (RF-MRB)

of the link, it can implement the optimal maximum ratio beamforming (MRB) solution. For this reason, in this paper we will refer to this architecture as RF-MRB (i.e., radio-frequency maximum ratio beamforming). A drawback of the RF-MRB topology is that the average power can vary widely across antennas, which is undesirable for the amplifiers since it can decrease their efficiency [3]. In order to mitigate this problem, in this paper we investigate an alternative radio-frequency equal gain beamforming (RF-EGB) scheme, which substitutes the vector modulators along each branch by analog phase shifters. Specifically, we focus on the optimization problem that results from this beamforming architecture.

For flat-fading single-input multiple-output (SIMO) or multiple-input single-output (MISO) channels, the equal gain beamformers that maximize the signal-to-noise (SNR) ratio are given by the phases of the SIMO or MISO channel, respectively [4]. For flat-fading MIMO channels, however, the optimization problem is nonconvex and no closed-form solution is known. Recently, Zheng et. al. have proposed in [5] an alternating minimization algorithm for the flat-fading MIMO case that uses the SIMO and MISO closed-form solutions iteratively by fixing one side of the link and solving for the other. Under OFDM transmissions the optimization problem becomes more challenging, since now we have to optimize a global measure of performance (typically the SNR) using a common set of Tx-Rx phases for all subcarriers. Building upon [5] and our own previous work in [6,7,8], the main contribution of this paper is to provide a suboptimal solution for this optimization problem and study its performance by means of simulations.

This paper is organized as follows. In Section 2 we present the analog MIMO beamforming architecture based on phase shifters. In Section 3 we summarize the EGB algorithm for flat-fading MIMO channels proposed in [5]. Section 4 contains the main contribution of this paper, which is the approximate maximum SNR solution for the RF-EGB architecture under OFDM transmissions. In Section 5 we compare the performance in 802.11a WLAN systems of the proposed RF-EGB beamforming architecture with the RF-MRB, the full-baseband MIMO and the SISO schemes. Finally, the main conclusions are summarized in Section 6.

1.1 Notation

Bold upper and lower case letters denote matrices and vectors respectively; light-faced lower case letters denote scalar quantities. We use $(\cdot)^H$, $(\cdot)^T$ and $\|\cdot\|$ to denote Hermitian, transpose and the Frobenius norm, respectively. $\mathbf{v}_{max}(\mathbf{A})$ is the principal eigenvector of the Hermitian semidefinite positive matrix $\mathbf{A}$. We use $\mathrm{dist}(\mathbf{x}, \mathbf{y})$ to denote the Euclidean distance between vectors $\mathbf{x}$ and $\mathbf{y}$. The vector formed by the phase angles of $\mathbf{x}$ is denoted as $\angle\mathbf{x}$. Finally, the expectation operator is denoted as $E[\cdot]$.

2 Proposed RF-EGB Architecture

The RF-EGB MIMO architecture studied in this paper is schematically shown in Fig. 2. Essentially, the vector modulators in Fig. 1 are now substituted by wide-band analog phase shifters. In this way, we avoid the power imbalance among the various antenna branches and the wide power variations that can happen in maximum ratio beamforming schemes. As long as the gains of the amplifiers of the various branches match, the rest of the parameters can be relaxed and inexpensive amplifiers can then be utilized. We consider WLAN 802.11a transmissions [9] that use orthogonal frequency division multiplexing (OFDM) and achieve a data transmission of up to 54 Mbps. It is important to mention here that the RF-EGB architecture does not try to solve the PAPR (peak-to-average power ratio) problem of OFDM modulations, it just avoids power variations among the analog signal paths. To mitigate this important problem of OFDM systems, we could apply one of the many proposed PAPR reduction techniques [10] or operate the amplifiers with some back-off.

It is also assumed that both the transmitter and the receiver have perfect channel state information, which has been obtained using specifically designed training sequences. The system is intended for low-mobility indoor scenarios as those encountered in WLAN transmissions, therefore we consider that the channel remains static during the transmission of several frames. More details about the training procedure and other implementation aspects of RF-MIMO transceivers can be found in [1,2] and the references therein.

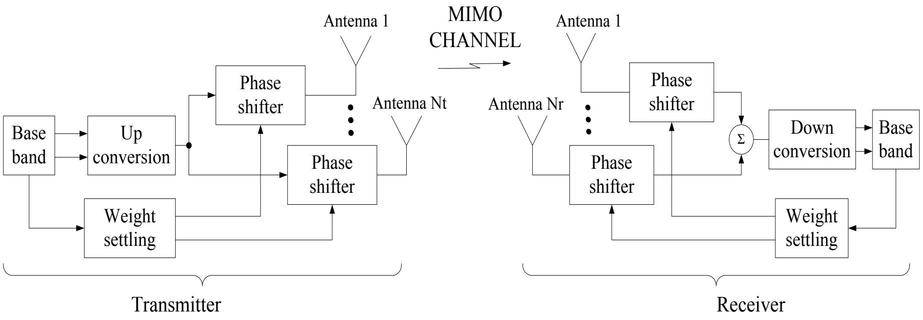


Fig. 2. Equal gain beamforming in the radio-frequency domain (RF-EGB)

The RF-EGB architecture poses several implementation challenges. For instance, it can be difficult to design wideband phase shifters achieving a constant phase change without any amplitude variation over the 20 MHz bandwidth required in WLAN 802.11a transmissions. Also, the automatic gain control system at the receiver side can affect the equal gain beamforming. To simplify the analysis, however, in this paper we will consider an idealized system in which all these circuitry impairments are neglected, and we will focus just on the optimization problem.

3 RF-EGB Solution for Flat-Fading MIMO Channels

In this section we describe the baseband model for MIMO beamforming schemes, and summarize the iterative EGB solution proposed in [5] for flat fading MIMO channels. Let us consider an $N_r \times N_t$ MIMO system with N_t transmit and N_r receive antennas. The unit-norm transmit and receive beamformers are $\mathbf{w}_t = (w_{t,1} w_{t,2} ... w_{t,N_t})^T$ and $\mathbf{w}_r = (w_{r,1} w_{r,2} ... w_{r,N_r})^T$, respectively. Although these beamformers are implemented in the RF domain, we can use the conventional baseband model for the received signal

$$y = \mathbf{w}_r^H \mathbf{H} \mathbf{w}_t s + \mathbf{w}_r^H \mathbf{n},$$

where $s \in \mathbb{C}$ is the transmitted symbol, $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$ is the flat-fading MIMO channel matrix, and $\mathbf{n} \in \mathbb{C}^{N_r \times 1}$ is the noise vector, whose entries are independent identical distributed (i.i.d.) complex Gaussian random variables with zero-mean and variance σ_n^2.

Notice that using MIMO beamforming the symbols are transmitted through an equivalent SISO channel: $h = \mathbf{w}_r^H \mathbf{H} \mathbf{w}_t$. Assuming now that the transmitted sequence has unit power, the receive SNR is given by

$$\mathrm{SNR} = \frac{E\left[\left|\mathbf{w}_r^H \mathbf{H} \mathbf{w}_t s\right|^2\right]}{E\left[\left|\mathbf{w}_r^H \mathbf{n}\right|^2\right]} = \frac{\left|\mathbf{w}_r^H \mathbf{H} \mathbf{w}_t\right|^2}{\sigma_n^2} \,. \tag{1}$$

With maximum ratio beamforming we obtain the beamformer weights (amplitudes and phases) that maximize the receive SNR given by (1). As it is well-known, this maximization problem has a closed-form solution which is given by the left and right singular vectors corresponding to the largest singular value of $\mathbf{H}$ [11]. However, for equal gain beamforming an additional constraint must be added to the problem: the elements of the transmit and receive beamformers have a constant modulus, $1/\sqrt{N_t}$ for $\mathbf{w}_t$, and $1/\sqrt{N_r}$ for $\mathbf{w}_r$. Therefore, the SNR maximization problem with EGB can be formulated as

$$\max_{\{\mathbf{w}_r, \mathbf{w}_t\}} \left|\mathbf{w}_r^H \mathbf{H} \mathbf{w}_t\right|^2 \tag{2}$$

$$\begin{aligned} \text{subject to : } \left|\mathbf{w}_{r,i}\right|^2 &= \frac{1}{N_r}, \qquad & i = 1, 2, \ldots, N_r, \\ \left|\mathbf{w}_{t,j}\right|^2 &= \frac{1}{N_t}, \qquad & j = 1, 2, \ldots, N_t. \end{aligned}$$

This is a nonconvex optimization problem which has no known closed-form solution. In [5] this problem is solved by means of a cyclic algorithm. First, it is shown that, unlike the MIMO case, for MISO and SIMO channels the equal gain beamforming problems have the following well-known closed-form solutions [4]

$$\mathbf{w}_t = \frac{e^{j\angle \mathbf{h}_{\mathrm{MISO}}{}^H}}{\sqrt{N_t}}, \qquad \mathbf{w}_r = \frac{e^{j\angle \mathbf{h}_{\mathrm{SIMO}}}}{\sqrt{N_r}} . \tag{3}$$

where $\mathbf{h}_{\mathrm{MISO}} \in \mathbb{C}^{1\times N_t}$ and $\mathbf{h}_{\mathrm{SIMO}} \in \mathbb{C}^{N_r\times 1}$ are the MISO and SIMO channel vectors, respectively. By exploiting this result, the equal gain beamformers for the MIMO case are obtained in [5] applying an alternating minimization approach as follows:

1. **Step 0:** Initialize $\mathbf{w}_r$ as the left singular vector of $\mathbf{H}$ corresponding to its largest singular value.
2. **Step 1:** Fix $\mathbf{w}_r$ and obtain $\mathbf{w}_t$ as the solution of the MISO case by taking $\mathbf{h}_{\mathrm{MISO}} = \mathbf{w}_r\mathbf{H}$ as the effective (equivalent) MISO channel

$$\mathbf{w}_t = \frac{e^{j\angle \mathbf{H}^H \mathbf{w}_r}}{\sqrt{N_t}} . \tag{4}$$

3. **Step 2:** Fix $\mathbf{w}_t$ and obtain $\mathbf{w}_r$ as the solution of the SIMO case by taking $\mathbf{h}_{\mathrm{SIMO}} = \mathbf{H}\mathbf{w}_t$ as the effective SIMO channel

$$\mathbf{w}_r = \frac{e^{j\angle \mathbf{H}\mathbf{w}_t}}{\sqrt{N_r}} . \tag{5}$$

Iterate steps 1 and 2 until a given stop criterion is satisfied, in our case we proposed to use the Euclidean distance between two consecutive beamformers

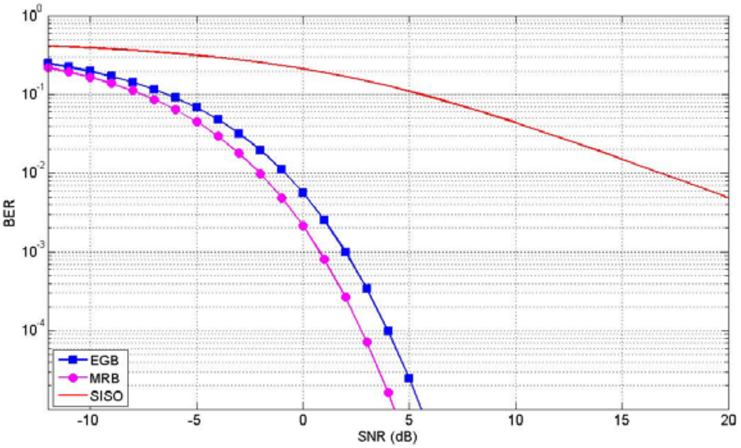


Fig. 3. Bit error rate comparison for EGB and MRB. QPSK symbols.

as the stop criterion. Specifically, the algorithm is stopped when the following two conditions are simultaneously satisfied:

$$|\mathrm{dist}(\mathbf{w}_{t,k}, \mathbf{w}_{t,k-1})| < \mathrm{dist}_{\max} \quad \text{and} \quad |\mathrm{dist}(\mathbf{w}_{r,k}, \mathbf{w}_{r,k-1})| < \mathrm{dist}_{\max}, \tag{6}$$

where k denotes iteration and $\mathrm{dist}_{\max}$ is the maximum error allowed. As an example of its performance, we show in Fig. 3 a comparison between MRB and EGB for a 4x4 Rayleigh flat-fading MIMO channel. It is clear that EGB attains the same spatial diversity than MRB, although we are losing part of the array gain, about 1.2 dB in this particular example.

4 RF-EGB Solution for OFDM-MIMO Channels

Under OFDM transmissions, the RF-EGB optimization problem becomes even harder due to the coupling among subcarriers. In fact, this problem is closely related to the design of pre-FFT schemes, which have been proposed to reduce the computational cost of conventional OFDM-MIMO transceivers [12,**?**]. However, these pre-FFT techniques are applied in the baseband and typically optimize the amplitudes and phases, therefore they are not directly applicable to our system.

Assume an OFDM transmission scheme with N_c data carriers and with a cyclic prefix longer than the channel impulse response and let $\mathbf{H}_k \in \mathbb{C}^{N_r \times N_t}$ be the MIMO channel for the k-th data-carrier. After analog Tx-Rx beamforming, at each carrier we have an equivalent SISO channel given by

$$h_k = \mathbf{w}_r^H \mathbf{H}_k \mathbf{w}_t, \qquad k = 1, \ldots, N_c \; .$$

Our goal is to find the equal gain Tx-Rx beamformers maximizing the overall receive SNR, i.e.,

$$\mathrm{SNR} = \frac{\sum_{k=1}^{N_c} \left|\mathbf{w}_r^H \mathbf{H}_k \mathbf{w}_t\right|^2}{\sigma_n^2} \; . \tag{7}$$

Therefore we can pose the RF-EGB SNR maximization problem as follows

$$\begin{aligned} &\max_{\{\mathbf{w}_r, \mathbf{w}_t\}} \sum_{k=1}^{N_c} \left|\mathbf{w}_r^H \mathbf{H}_k \mathbf{w}_t\right|^2 \\ \text{subject to : } &\left|\mathbf{w}_{r,i}\right|^2 = \frac{1}{N_r}, \qquad i = 1, 2, \ldots, N_r \\ &\left|\mathbf{w}_{t,j}\right|^2 = \frac{1}{N_t}, \qquad j = 1, 2, \ldots, N_t. \end{aligned} \tag{8}$$

To obtain a suitable solution to this problem, we suggest a cyclic algorithm inspired by the one previously described for the flat-fading case in Section 3. In the next subsection we first propose a closed-form (but suboptimal) solution for the frequency-selective MISO/SIMO cases.

4.1 EGB for Frequency-Selective MISO/SIMO Channels

For a MISO channel, the problem (8) is reduced to

$$\max_{\{\mathbf{w}_t\}} \sum_{k=1}^{N_c} \left| \mathbf{h}_{\mathrm{MISO}k} \mathbf{w}_t \right|^2 \tag{9}$$

$$\text{subject to} : \left|\mathbf{w}_{t,i}\right|^2 = \frac{1}{N_t}, \qquad i = 1, 2, \ldots, N_t$$

where $\mathbf{h}_{\mathrm{MISO}k} \in \mathbb{C}^{1 \times N_t}$ is the MISO channel vector for the k-th carrier. In order to derive a suboptimal solution for this problem let us rewrite (9) as

$$\max_{\{\mathbf{w}_t\}} \mathbf{w}_t^H \mathbf{R}_{\mathrm{MISO}} \mathbf{w}_t \tag{10}$$

$$\text{subject to} : \left|\mathbf{w}_{t,i}\right|^2 = \frac{1}{N_t}, \qquad i = 1, 2, \ldots, N_t$$

where

$$\mathbf{R}_{\mathrm{MISO}} = \sum_{k=1}^{N_c} \mathbf{h}_{\mathrm{MISO}}{}_k^H \mathbf{h}_{\mathrm{MISO}k} \ .$$

Again, the max-SNR problem for the MISO case in Eq. (10) is a complicated nonconvex problem with no closed-form solution. In this paper we propose to use the following simple, yet accurate, approximate solution given by the phases of the principal eigenvector of $\mathbf{R}_{\mathrm{MISO}}$

$$\mathbf{w}_t = \frac{1}{\sqrt{N_t}} e^{j\angle \mathbf{v}_{max}(\mathbf{R}_{\mathrm{MISO}})} \ . \tag{11}$$

This solution is motivated by the fact that the main eigenvector of $\mathbf{R}_{\mathrm{MISO}}$ contains most of the channel energy averaged across carriers and, in consequence, its phases should be close to the optimal solution of (10). In the simulation section we will show some results supporting this claim.

Analogously, the solution for the SIMO case is given by

$$\mathbf{w}_r = \frac{1}{\sqrt{N_r}} e^{j\angle \mathbf{v}_{max}(\mathbf{R}_{\mathrm{SIMO}})} \ , \tag{12}$$

where $\mathbf{R}_{\mathrm{SIMO}} = \sum_{k=1}^{N_c} \mathbf{h}_{\mathrm{SIMO}n} \mathbf{h}_{\mathrm{SIMO}}{}_n^H$.

4.2 Alternating minimization Algorithm

Inspired by the cyclic algorithm in [5], which was summarized in Section 3, we solve the SNR maximization problem in (8) as follows

1. **Step 0:** Initialize $\mathbf{w}_r$ (e.g., to a random value).
2. **Step 1:** Consider $\mathbf{w}_r$ fixed and take $\mathbf{h}_{\mathrm{MISO}k} = \mathbf{w}_r^H \mathbf{H}_k$ as the equivalent MISO channel for each subcarrier. The solution for $\mathbf{w}_t$ is then given by (11).
3. **Step 2:** With $\mathbf{w}_t$ fixed to the value obtained in the previous step, construct the equivalent SIMO channels as $\mathbf{h}_{\mathrm{SIMO}k} = \mathbf{H}_k \mathbf{w}_t$ and obtain the solution for the receive equal gain beamformer as (12).

Steps 1 and 2 are iterated until the criterion defined in (6) is satisfied.

5 Simulation Results

In this section, we evaluate the performance of the proposed algorithm by means of numerical simulations in MATLAB. For all simulations we consider a Rayleigh 4x4 MIMO channel model with an exponential power delay profile parameterized by ρ, i.e.,

$$E\left[\|\mathbf{H}[l]\|^2\right] = \rho^l \frac{1-\rho}{1-\rho^L} N_r N_t \qquad l = 0, \ldots, L-1,$$

where $L = 16$ is the length of the channel impulse response which is assumed to be equal to the cyclic prefix length. To check the convergence of the algorithm we use a maximum error of $\mathrm{dist}_{\max} = 10^{-3}$ (see Eq. (6)).

To verify the goodness of our method we first study how far is the proposed suboptimal solution from the optimal one obtained by means of a brute-force search. To this end we consider simple 1×2 and 1×3 MISO systems and evaluate the energy of the equivalent SISO channel, $\sum_{k=1}^{N_c} \mid \mathbf{h}_{\mathrm{MISO}k} \mathbf{w}_t|^2$, for both the suboptimal and optimal solutions. For high frequency-selective channels (i.e., $\rho = 1$), we found that the optimal equal-gain beamformer outperforms our suboptimal solution by less than 10^{-3} dB and 10^{-2} dB for the 1×2 and 1×3 MISO channels, respectively. In addition, we found that as the channel becomes less frequency selective our suboptimal solution gets even closer to the optimal one. This support our claim that the proposed method provides a good approximation of the optimal equal-gain beamforming phases.

Now, we compare the performance of the following methods:

1. RF-MIMO architecture with the proposed equal gain beamforming algorithm (RF-EGB).
2. RF-MIMO architecture with maximum ratio beamforming (RF-MRB)
3. Conventional baseband MIMO-OFDM system with optimal (per-carrier) maximum ratio beamforming (Full-MIMO)
4. SISO system.

For the RF-MRB architecture we apply the maximum SNR solution obtained with the algorithm described in [8]. The Full-MIMO and the SISO schemes can be seen as the upper and lower bounds, respectively, for the performance of any system. For these simulations ρ has been fixed as $\rho = 0.7$, which represents a high frequency-selective MIMO channel.

We consider coded and uncoded transmissions with frames generated according to the 802.11a WLAN standard [9] (OFDM symbols with 64 carriers, out of them 48 are data carriers, 4 are pilots and the rest are unused). Nevertheless, let us remark that throughout this paper we have assumed perfect channel knowledge and therefore the pilots were not used for channel estimation. The impact of the channel estimation errors and other RF impairments is left for future work.

In the first simulation example we consider uncoded QPSK modulated data to be transmitted over the 48 data carriers. The bit error rate (BER) curves

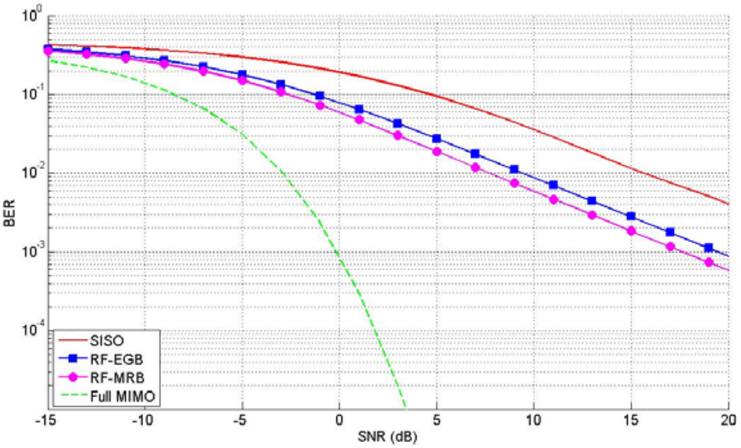


Fig. 4. Bit error rate vs. SNR for the compared algorithms. Uncoded QPSK symbols.

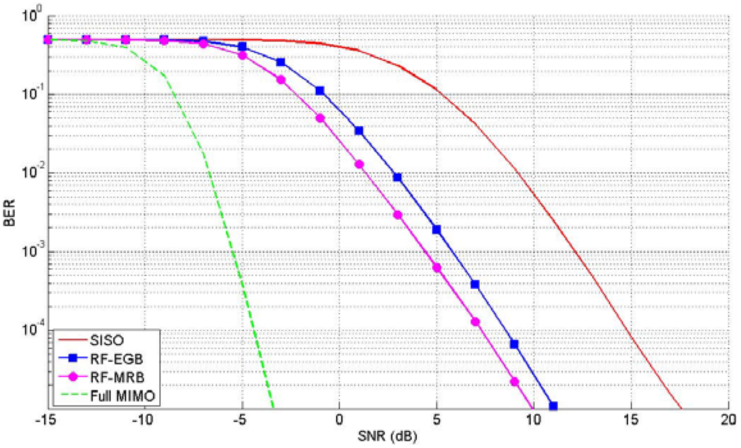


Fig. 5. Bit error rate for the compared algorithms. Coded QPSK symbols, R=1/2, 12 Mbps.

for the different methods are shown in Fig. 4. As we can observe, for uncoded transmissions and high frequency-selective MIMO channels, both RF-MIMO architectures fail to extract any or almost no frequency/spatial diversity, since the performance is limited by the worst subcarriers. Both schemes, however, achieve an important array gain in comparison to a SISO system. The RF-EGB performance is always inferior to the RF-MRB performance and the gap depends on the number of antennas and the frequency selectivity of the channel (i.e., ρ). For a BER=10^{-3} this loss is approximately 1.8 dB.

For the second example we have chosen a more realistic scenario using coded transmissions under the 802.11a standard for a 12 Mbps rate (QPSK modulation

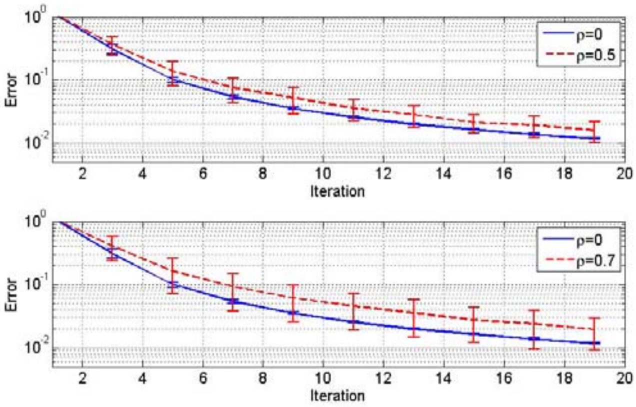


Fig. 6. Convergence of the algorithm for different values of ρ. 4x4 antenna configuration.

and a code rate of 1/2). The data bits are encoded with a convolutional code and block interleaved as specified in the 802.11a standard. The receiver is based on a hard decision Viterbi decoder. The results are shown in Fig. 5: with coded transmissions, both analog combining schemes are able to extract, at least partly, the frequency and spatial diversity of the channel, although there is still an important gap with respect to the Full-MIMO architecture. Nevertheless, as it has been shown in [6,7,8] this gap can be diminished by optimizing other cost functions (the mean square error, for instance) instead of the SNR. Obviously, MRB achieves better results than EGB; however, the difference for a BER=10^{-3} is about 1.4 dB. Again, this supports our claim that the approximate EGB solution proposed in this paper is close to the optimal one.

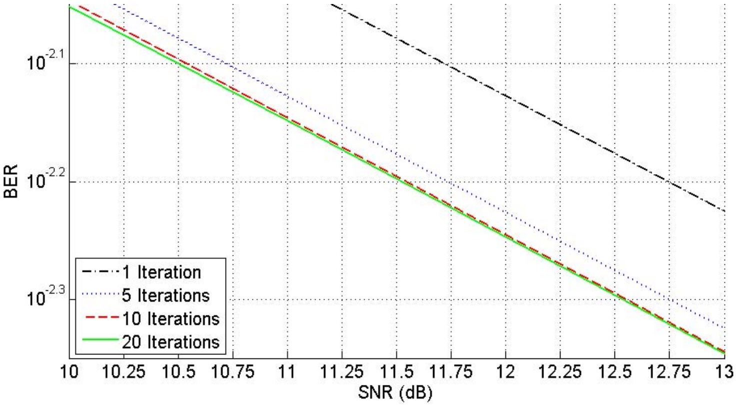


Fig. 7. BER curves for different number of iterations. 4x4 RF-EGB system, QPSK uncoded symbols and channel with $\rho = 0.7$.

In Fig. 6 we illustrate the convergence of the proposed alternating minimization algorithm for different values of ρ. These plots represent the Euclidean distance between beamformers obtained in two consecutive iterations. The convergence curves have been obtained by averaging 500 independent trials, and the vertical bars indicate the variance. Finally, Fig. 7 presents the evolution of the BER curves with the number of iterations in the SNR range of 10-13 dB. We can conclude that the algorithm converges very fast within the first 10 iterations, although the convergence speed decreases and the variance increases for larger values of ρ (i.e., for high frequency-selective channels).

6 Conclusions

MIMO transceivers performing spatial processing in the RF domain (RF-MIMO) are a good alternative in order to reduce the hardware cost and system size, as well as to increase the energy-efficiency of the system. In this paper we have studied a particular scheme (RF-EGB), which applies the equal gain combining concept and only uses phase shifters before the analog combiner, instead of full vector modulators as previously proposed (RF-MRB scheme). Under OFDM-WLAN transmissions, the proposed scheme results in a complicated optimization problem since the Tx-Rx analog equal gain beamformers simultaneously affects all subcarriers. We have proposed simple (but suboptimal) solutions for the MISO and SIMO cases, and based on these, a cyclic minimization algorithm to get the maximum SNR solution for the MIMO case. The proposed algorithm has been shown to provide good results with a low computational complexity, since it converges in very few iterations. Coded and uncoded data 802.11a transmissions have been simulated, and in both cases, RF-EGB has shown to behave only slightly inferior to the RF-MRB scheme.

Acknowledgment

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n 213952, MIMAX. The work of the fourth author has been supported by MAEC-AECID (Agencia Española de Cooperación Internacional para el Desarrollo).

References

1. Eickhoff, R., et al.: MIMAX: Exploiting the maximum performance and minimum system costs of wireless MIMO systems. In: 17th ICT Mobile and Wireless Summit, Stockholm, Sweden (2008)
2. Eickhoff, R., Kraemer, R., Santamaria, I., Gonzalez, L.: Integrated low power RF-MIMO transceiver for enhanced 802.11a short-range communication. IEEE Vehicular Technology Magazine, 34–41 (2009)

3. Ellinger, F.: Radio Frequency Integrated Circuits and Technologies. Springer, Berlin (2007)
4. Love, D.J., Heath, R.W.: Equal gain transmission in multiple-input multiple-output wireless systems. IEEE Trans. Commun. 51, 1102–1110 (2003)
5. Zheng, X., Xie, Y., Li, J., Stoica, P.: MIMO transmit beamforming under uniform elemental power constraint. IEEE Trans. Signal Process. 55, 5395–5406 (2007)
6. Via, J., Elvira, V., Santamaria, I., Eickhoff, R.: Analog antenna combining for maximum capacity under OFDM transmission. In: IEEE International Conference on Communications, Dresden, Germany (2009)
7. Via, J., Elvira, V., Santamaria, I., Eickhoff, R.: Minimum BER beamforming in the RF domain for OFDM transmissions and linear receivers. In: IEEE International Conference on Acoustics Speech and Signal Processing, Taipei, Taiwan (2009)
8. Via, J., Santamaria, I., Elvira, V., Eickhoff, R.: A general criterion for joint Tx-Rx beamforming in the RF domain under OFDM transmissions. IEEE Transactions on Signal Processing 58(4), 2155–2167 (2010)
9. IEEE Std. 802.11a, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHZ Band. IEEE (1999)
10. Van Nee, R., Prasad, R.: OFDM for wireless multimedia communications. Artech House, Norwood (2000)
11. Andersen, J.B.: Array gain and capacity for known random channels with multiple element arrays at both ends. IEEE Journal on Selected Areas in Communications 11, 2172–2178 (2000)
12. Rahman, M., Witrisal, K., Das, S., Fitzek, F., Olsen, O., Prasad, R.: Optimum pre-DFT combining with cyclic delay diversity for OFDM based WLAN systems. In: IEEE 59th Vehicular Technology Conference, vol. 4, pp. 1844–1848 (2004)
13. Li, S., Huang, D., Letaief, K., Zhou, Z.: Pre-DFT processing for MIMO-OFDM systems with space-time-frequency coding. IEEE Trans. on Wireless Comm. 6(11), 4176–4182 (2007)

A Framework for the Design Space Exploration of Software-Defined Radio Applications

Thorsten Jungeblut[1], Ralf Dreesen[3], Mario Porrmann[1], Michael Thies[3],
Ulrich Rückert[2], and Uwe Kastens[3]

[1] Heinz Nixdorf Institute, University of Paderborn, Germany
[2] Cognitive Interaction Technology - Center of Excellence, Bielefeld University, Germany
[3] University of Paderborn, Germany

Abstract. This paper describes a framework for the design space exploration of resource-efficient software-defined radio architectures. This design space exploration is based on a dual design flow, using a central processor specification as reference for the hardware development and the automatic generation of a C-compiler based tool chain. Using our modular rapid prototyping environment RAPTOR and the RF-frontend DB-SDR[1], functional verification of SDR applications can be performed. An 802.11b transmitter SDR implementation is mapped on our CoreVA VLIW architecture and evaluated in terms of execution time and energy consumption. By introducing application specific instruction set extensions and a dedicated hardware accelerator, execution time and energy consumption could be reduced by about 90 %.

Keywords: Design Space Exploration, Software-Defined Radio, Architecture, VLIW, CoreVA.

1 Introduction

Wireless communication more and more finds its way into our daily life. Mobile devices support complex applications, like high definition television(HDTV), video conferences, or online gaming. Simultaneously, new mobile transmission protocols allow higher throughput and lower latencies. Furthermore, the computational demand of these protocols increases steadily. Instead of using multiple dedicated hardware components for each algorithm, the trend is towards single, reconfigurable, general purpose processing units. The higher integration rate of microelectronic devices allows CPUs to support the required processing power at reasonably low energy consumption. In the beginning of the 1990's, Joe Mitola coined the term *Software Radio Architecture* or *Software-Defined Radio*. In [8] he defines software radio as a set of Digital Signal Processing (DSP) primitives, a metalevel system for combining the primitives into communications systems functions (transmitter, channel model, receiver, . . .) and a set of target processors on which the software radio is hosted for real-time communications. Software

---

[1] DB: daughter board, SDR: software-defined radio.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 148–159, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

radio adds the flexibility to the communication systems to allow the dynamic reconfiguration of the used standards. In case of changes in the standards, updates can be performed by simple software updates. Modifications of hardware components are not necessary. High level programming languages like C/C++ make development of the applications hardware independent and more maintainable. Fine grained reconfigurable devices like *Field Programmable Gate Arrays (FPGA)* add additional computational power for highly parallelizable signal processing components. In addition, the general purpose CPU is not only suitable to execute radio-based algorithms, but also the operation system or multimedia applications. The complexity of the radio architecture is highly reduced.

This work presents a framework for the development and design space exploration of software-defined radio applications. Both software application and hardware platform are taken into account. In Section 3 we present a holistic tool flow for the evaluation of the resource efficiency of the hardware-/software combination. The tool flow is based on a central processor specification described in the UPSLA language[6], which acts as a reference for the development of the hardware and the software development tools. In Section 3 we introduce the CoreVA VLIW architecture which plays the role of the central general purpose CPU to execute the radio protocols. In Section 4 we present our rapid prototyping environment RAPTOR, a modular architecture for the evaluation and verification of the radio application. The flexible software-defined radio extension module *DB-SDR* is used for the realization of the RF-parts of the software radio architecture. In Sections 5 and 6 we discuss the potential of our tool flow by mapping a IEEE 802.11b transmitter SDR implementation to our CoreVA architecture and present the results of the optimization by application specific instruction set extensions and hardware accelerators. In Section 7 we conclude our work and propose potential optimizations and future extensions.

2 Related Work

In [7] Joe Mitola describes the potential of a software radio architecture and the necessity of open architecture interface standards (e.g. Common Object Resource Broker (CORBA)). The architecture is defined as a comprehensive, consistent set of functions, components, and design rules. A channel stream is partitioned into five segments : *Antenna Segment*, *IF Processing Segment*, *Baseband Processing Segment*, *Bitstream Segment*, and *Source Segment*. The author presents an estimation of resource requirements. The highest computational demand (>1 billion operations per second) relates to the IF Processing Segment. He takes for example a bandwidth of 10 MHz and a oversampling sampling factor of 2.5. With a computational demand of 100 operations per sample this sums up to 2.5 billion operations per second. To handle the complexity, he suggests to assign parts of the IF Processing Segments to heterogeneous multiprocessing hardware or dedicated chips as well.

[1] presents a tunable software-defined radio receiver from 800 MHz to 5000 MHz implemented in a 90 nm technology. The receiver chip size is $7\,mm^2$

and is sufficient to implement mobile standards from GSM up to 802.11g wireless LAN (up to 40 MHz sample rate).

The authors of [2] describe a programmable baseband platform for mobile and wireless LAN standards. The architecture embeds four single-instruction multiple data (SIMD) DSP cores which are accompanied by dedicated programmable processors for channel en-/decoding and filtering operations and an ARM processor for the execution of the protocol stack. To prove the feasibility of their approach, they investigated IEEE 802.11b as the first communication standard. The architecture operates at a frequency of 300 MHz.

In [10] and [11] a software defined radio prototype based on a multiprocessor architecture is proposed. Several mobile applications as well as IEEE 802.11b wireless LAN is implemented. They use flexible-rate pre-/post-processors, four TMS320C6201 DSPs (200 MHz) and a PowerPC (400 MHz) to handle bandwidths of up to 20 MHz. User data rates of up to 2 MBit/s (IEEE 802.11b, DQPSK) are achieved.

In [4] Intel targets wireless LAN standards in the 802.11 series with its reconfigurable communications architecture embedding a mesh of processing elements and couples to analog front ends implemented in a CMOS technology.

All approaches show the immane computational demand required for baseband processing and the enlargement of the design space to be considered. Our methodology allows a fast and accurate evaluation of SDR based applications.

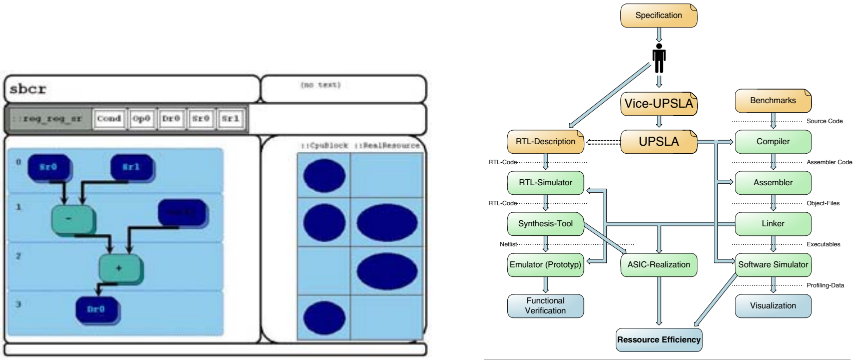
3 Processor Design Based on UPSLA

For development of processor architectures and the corresponding tool chains we use a dual design flow based on the Unified-Processor-Specification-Language (UPSLA) as a reference description (cf. Figure 1b).

UPSLA is a declarative language for the description of processor architectures. The language uses object oriented techniques, which leads to a very compact specification. For sharing of common properties inheritance can be used. Instances with the same behavior are grouped into equivalence classes. This avoids redundancy and enables consistent, global changes on the specification. By this the processor specification can easily be adapted to changes in the architecture. UPSLA is described in textual form. This can be done manually or by a graphical user interface (ViceUPSLA, cf. Figure 1a).

Based on this specification, a complete tool chain can be generated automatically. The tool chain consists of a C-compiler, an assembler, a linker, an instruction set simulator and various debugging and profiling tools.

As a result of this profiling, modifications to the processor architectures can be performed, for example by modifying the instruction set or adding additional functional units (cf. Section 6, [5]). The consistency of the generated tool chain and the hardware description is checked using a validation by simulation approach presented in [3]. Functional verification is performed using our rapid prototyping environment RAPTOR resented in Section 4.



(a) ViceUPSLA for the graphicalesription of the processor specification

(b) The central processor specification in the UPSLA languagects as a reference for the hardware development and the software tool chain

Fig. 1. Dual design flow for the development of processor architectures

The CoreVA architecture. The CoreVA architecture represents a 4-issue VLIW architecture[5]. Using the hardware description language VHDL, CoreVA is specified as a soft macro at register-transfer-level (RTL). The typical harvard architecture with separated instruction and data memory provides a six-staged pipeline (instruction fetch (FE), instruction decode (DE), register read (RE), execute (EX), memory (ME), and register write (WR).

Besides four arithmetic-logical-units (ALUs), two dedicated multiply-accumulate (MLA) units support fast multiplication. Divisions are accelerated by two dedicated division step units. The register file comprises 31 general purpose 32-bit registers, which can be accessed by all four issue slots. The byte-wise addressable memory supports 8-bit, 16-bit and 32-bit data transmissions using natural alignment and little-endian byte-ordering. The operations follow a two- and three-address format and are all executed in one clock cycle. Most instructions have a latency of one clock cycle, except branch, MLA and load operations, which have a latency of two clock cycles. In SIMD (single instruction, multiple data) mode, two 16-bit words can be processed in each functional unit (FU), which leads to an eightfold parallelism. Two 7-bit condition registers support conditional execution for scalar and SIMD operations. If not all FUs can be utilized, a stop bit in the opcode allows to omit empty trailing instruction slots. This leads to more compact code and reduces power consumption, which is very useful for embedded systems, e.g. smart cards. Still, 64% of the opcode space of the CoreVA architecture are free and can be used for instruction set extensions. The CoreVA architecture operates at a clock frequency of 300 Mhz. Area consumption is about 4 mm^2 including 32 kByte Level-1 cache for instruction and data. The CoreVA architecture is implemented as a configurable IP-core, for example, the number of functional units, dedicated multipliers/dividers or load/store units can be specified.

4 A Flexible RF Frontend for SDR Applications

For the functional verification of the hardware implementation, we use the RAPTOR2000/X64 rapid prototyping environment [9]. This modular system offers a large selection of FPGA daughter boards or physical interfaces (e.g. Ethernet), which enable the use in real environments.

For the functional verification of software-defined radio applications, we developed an extension module for our RAPTOR family. This module is compatible to the USRP[2] base system and extension modules from Ettus Research[3]. Hereby the extension modules from Ettus Research can directly be reused an RF frontends need not to be developed. By two connectors, these modules can be plugged to the DB-SDR RAPTOR module.

The transceiver modules available from Ettus Research enable the DB-SDR to be used as an adequate RF-transceiver. In general a bandwidth of 30 MHz can be set up. The fully synchronous implementation enables *Multiple Input Multiple Output (MIMO)*. In contrast to the RX- and TX modules, the transceivers include oscillators to enable split frequencies operations. *Frequency hopping* is enabled by dedicated PLLs[4]. Beyond this, all transceiver modules include analog RSSI[5] measuring systems to get direct access to the received field strength. *Automatic Gain Control* is used for a level normalization at 70 dB. All transceiver modules are full duplex capable and the transmit power is adjustable. The receiver modules available at Ettus Research range from 50 MHz to 5 GHz. The Ettus RFX2450 covers frequencies ranging from 2.4 to 2.5 GHz and 4.9 to 5.9 GHz at a maximum transmit power of 100 mW (20 dBm).

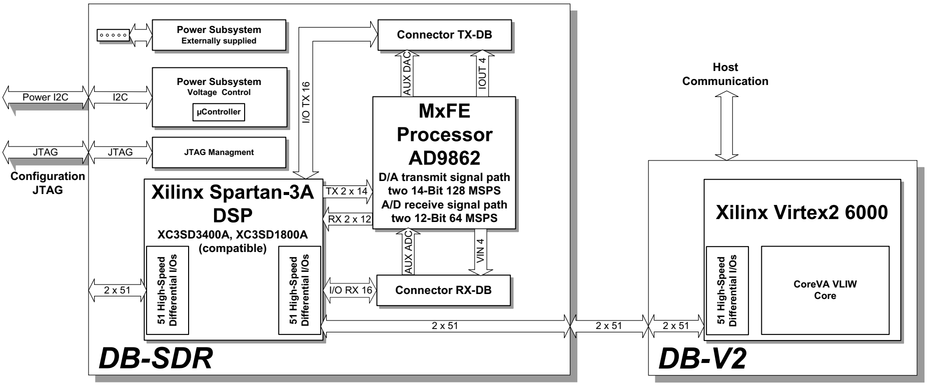


Fig. 2. Block diagram of the DB-SDR Extension module

---

[2] *U*niversal *S*oftware *R*adio *P*eripheral.

[3] http://www.ettus.com/

[4] PLL: Phase Locked Loop.

[5] RSSI: Received Signal Strength Indication.

AD/DA conversion. Core of the DB-SDR is the AnalogDevices AD9862. The AD9862 is a 12-/14 Bit *mixed signal front-end* (MXFE®) processor for broadband communication. The receive path consists of two 12 Bit A/D converters with a sample rate of 64 MSamples/s to sample a 32 MHz wide frequency band. The upper limit of the AD9862 is 100 MHz. The sending path consists of two high speed 14 Bit D/A converters. The clock frequency of the D/A converters is 128 MS/s, so the Nyquist frequency is 64 MHz. Additional PGAs allow an amplification of up to 20 dB. The outputs are current outputs of 0 to 20 mA. Beside this main AD/DA converters, the AD9862 embeds four *auxiliary analog inputs* with a 10 Bit *low-speed* A/D converter (1.25 MS/s, bandwidth of ≈ 200 KHz). This auxiliary analog inputs can be used for example to sample the RSSI signal levels or measuring of temperature or bias. An *low speed* 8 bit D/A converter can be used for example to control external amplifiers.

FPGA. The data preprocessing and the communication with the host system is performed by an Spartan 3 ADSP (XC3SD3400A or XC3SD1800A). This FPGA is also used to configure the AD9862 AD/DA converter and the extension modules by Ettus Research. An UART interface can be used for debugging.

Power management. The power can be supplied by the RAPTOR base board or externally to decouple noise from the host system. A Microship *PIC (Peripheral Interface Controller)* PIC18F6722 controls the initialization of the different voltages.

Clock distribution. Similar to the power supply, the reference clock for the AD/DA converter can be supplied externally or by a CTX286LVCT oscillator. The clock distribution is performed by an Analog Devices AD9513.

5 Case Study: Optimization of an IEEE 802.11b Transmitter SDR Implementation

In this section we will introduce a IEEE 802.11b related physical layer WLAN algorithm. The algorithm is implemented in C-Code and can be executed on our CoreVA architecture. The software processes MAC packets from the higher layers. The output is the discrete representation of the baseband signal to be transferred. Using a R/F-frontend as described in 4, the data is D/A converted and mixed to the ISM[6]-band and send to the receiver. The protocol is compatible to the algorithms of the GNU-Radio[7]. For sake of simplicity we only describe the transmitter part of the 802.11b standard in this section.

The implementation of the data path of the IEEE 802.11b algorithm consists of four function blocks (cf. Figure 3):

- Scrambler
- Differential Encoder

---

[6] Industrial Scientific Medical.

[7] http://www.gnuradio.org/

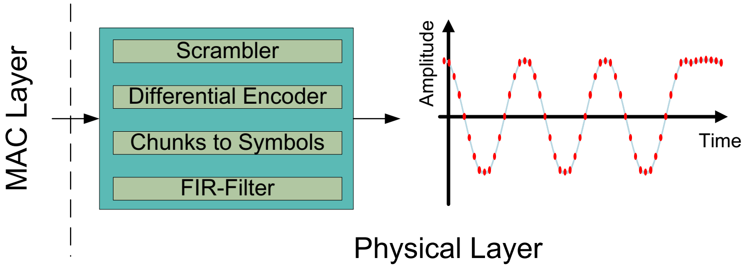


Fig. 3. Function blocks of the IEEE 802.11b algorithm

- Chunks to Symbols
- Interpolation FIR Filter

To enable clock recovery at the receiver, the transmitted signal must not contain long non-constant sequences. In the *Scrambler* the data is scrambled in a way which can be recovered by implementing a linear feedback shift register (LFSR). During the transmission the phase of the signal can be shifted by interference on the channel or by loss of synchronization between transmitter and receiver. If the phase exceeds a threshold a phase ambiguity emerges and the receiver misinterprets the received symbols. In BSPK coding, this effect emerges at phase shifts of more than $+90°$ and less than $-90°$. In QPSK misinterpretation can occur at shifts of $\pm 45°$ because of the fewer distance of the symbols. The *Differential Encoder* avoids these faults in advance by adding dependencies between the current and the subsequent bit. The output of the scrambler is combined bitwise by a modulo-2 operation to the last computed bit. By this only differences of consecutive bits are transferred. If two consecutive bits differ, a 1 is transferred, otherwise a 0. If a continuously phase shift occurs, the interpretation of the symbols might change but the dependencies can be restored in the receiver. Within the function block *Chunks to Symbols* the output of the differential encoder are mapped to the BPSK symbol space of IEEE 802.11b with a phase offset of $\frac{\pi}{4}$. The *Interpolation FIR(Finite Impulse Response)-Filter* converts symbols of the previous blocks to discrete values of the later analog transferred signal. The discrete values are characterized by the property, that a logical 0 is represented by amplitude of 0.361 and a logical 1 is represented by amplitude of -0.361. This signal implies a very wide frequency spectrum due to very steep edges. Thus it cannot be transferred efficiently. For this reason, the signal is shaped with a pulse, to apply to the ISM band. In time division, this pulse shaping is characterized by an interpolation, at which intermediate values are inserted to filter the edges. For the pulse forming, IEEE 802.11b uses the first half wave of a Root-Raised-Cosine function, which is based on an extended Sinus Cardinalis(SI)-function. The Root-Raised-Cosine function has the advantage, that a filter based on it meets the first nyquist criterion. In this work, the pulse forming is realized by a FIR filter of first order and implemented by a matrix multiplication of a vector containing the two subsequent symbols and the so called taps matrix. The taps matrix contains the discrete values of the root-raised-cosine. The number of columns complies with the order of the filter, the number of rows defines the interpolation rate. In this work, an interpolation rate of 8 is set. The result is a vector containing 8 discrete interim values. The matrix is initialized with a root-raised-cosine pulse with a roll-off-factor of 0.5.

Performance Results. The total execution time of the baseband processing of the IEEE 802.11b transmitter SDR implementation for a minimal packet (6 bytes payload of the PLCP frame $\widehat{=}$ 512 bytes baseband data) is 21100 clock cycles. At a clock frequency of 300 MHz this implies a processing time of $70\,\mu s$. The `Interpolation FIR Filter` consumes the most computation time (88 %) and is examined in particular in the optimization steps described in Section 6 (Scrambler: 4.5 %, Differential Encoder: 3 %, Chunks to Symbols: 4 %)

6 Example of Design Space Exploration

This section describes the optimization of the IEEE 802.11b transmitter SDR implementation introduced in Section 5. As the algorithm is intended to be executed on our CoreVA architecture on a mobile, energy limited device, we consider the optimization of resource consumption in terms of energy, so first and foremost we try to reduce execution time and power consumption.

The optimization process is divided into three independent intermediate steps affecting different domains of the hardware/software combination:

- Starting from the C-Reference Code, we adapt the implementation of the software to enable the compiler using architecture dependent parameters.
- Analyzing the instruction streams to introduce tightly coupled, application specific instruction set extensions (ISE) to the processor core.
- Adding loosely coupled dedicated hardware extensions

6.1 Optimizing the C-Code

Despite the fact, that a developer expects from an "ideal" compiler to convert C-code with the same behavior to identical (and optimal) machine code, reality does not look the same. The way of describing the functionality of the algorithm impacts the quality of the results. One reason (especially when using parallel systems like VLIW) is that compiling is always a tradeoff between code quality and compiler effort (compile time). On the other hand different implementations of an algorithm supposed to be obviously identically turn out to be different and have a great impact on the compilation result. One example is the non equivalence of `logical shift left` and `division by a power of two` when not using *unsigned* variables. Using variables not adapted to the width of the data path can force the compiler to insert additional instructions to handle overflows, even if this cannot occur with the set of input values used later. Manual unrolling of loops can improve speed, if the compiler cannot prove a fixed number of iterations during compile time. Aligning structures to memory boundaries can reduce clock cycles to calculate memory addresses, on the other hand, this often leads to a tradeoff between performance and memory requirements (In addition, the setup and output delays of a memory macro scales with its size and hereby can impact the maximum frequency of the total system.). Considering these rules the execution time of the IEEE 802.11b algorithm could be reduced by 25 %. Using the evaluation applications of our tool flow allows quick iteration steps in the design space exploration. For example, at this point of optimization, no modifications to the hardware had to be made. The resulting C-code is still portable to other architectures, and most of the modifications would produce performance gains on similar architectures, as well.

6.2 Introducing Instruction Set Extensions

Successive instructions with data dependencies can be combined to one single instruction. These instructions are derived directly from the evaluation applications of our tool flow. As such instruction sequences base on existing fundamental operations of the functional units, their combination often requires a negligible amount of additional hardware resources. For the proposed IEEE 802.11b transmitter SDR implementation, an `Multiply Accumulate` instruction is followed by a data dependent `arithmetic shift right` in 2304 clock cycles. After introducing an extension to the instruction set, the application could be sped up by about 4 %. The critical path of the architecture is not affected. The increase in area and power consumption is negligible and below the variations of non deterministic synthesis processes. As execution time is reduced the required energy for the processing of the algorithm is reduced analogously (cf. Figure 4). Following this example several candidates of instruction pairs can be implemented to further improve the energy balance.

6.3 Loosely Coupled, Dedicated Hardware Extensions

Moving from general purpose optimization methods not exclusively suited for the IEEE 802.11b application, the next step is to introduce dedicated hardware extensions, to which whole parts of the algorithms can be migrated to. Usually, these extensions have higher performance but increased resource requirements compared to instruction extensions. As before, the developer has to consider this tradeoff for example by considering the required energy as a ranking measure. In the example presented in this section, we implemented a hardware accelerator for the processing of 802.11b MAC packets. The packets are transferred to the hardware extension, processed by four dedicated components representing the four components of the reference software implementation described in Section 5 (cf. Figure 5).

The combinatorial logic is decoupled by input and output registers to avoid impacts on the critical path of the processor core. Address decoders control the distribute the data from the CPU to the internal registers of the hardware

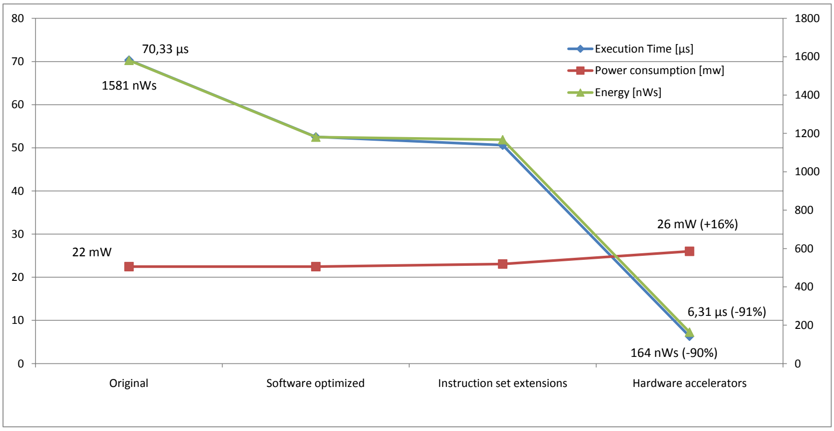


Fig. 4. Optimization results for the IEEE 802.11b transmitter SDR implementation

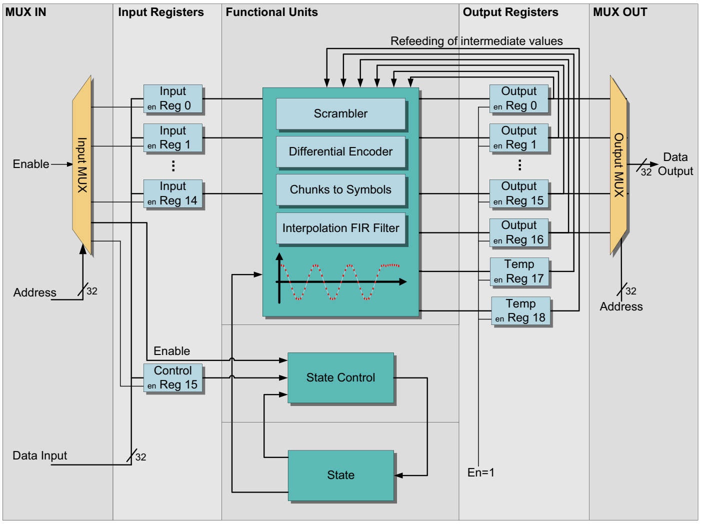


Fig. 5. Block diagram of the IEEE 802.11b hardware accelerator

extension and vice versa. All parts of the hardware extension share the same internal registers for intermediate data. A state machine controls the access to the registers and the processing of the data. The execution time for the processing of a data byte is 5 clock cycles. The final results of the computations are the discrete signal values transferred to the physical layer. The maximum clock frequency of the system including the hardware accelerator is not affected. The area requirements are increased by about 32 %, the power consumption by about

16 %. The execution time of IEEE 802.11b algorithm using the hardware accelerator is reduced by about 90 %. Figure 4 depicts the optimization results the presented optimization steps. By adding the hardware accelerators, the energy consumption could be reduced by about 91 %.

7 Conclusion

We presented a framework for the design space exploration and development of SDR architectures. This framework is based on dual design flow, consisting of the automatic generation of a complete C-compiler tool chain based on a high level reference specification in the UPSLA languagend a conventional RTL-based hardware development. We presented the CoreVA VLIW architecture for the execution of the baseband algorithms. Functional verification is performed using our rapid prototyping environment RAPTOR For this modular architecture a RF-frontend has been developed. This module can be extended with commercial RF-transceivers from Ettus Research. To demonstrate the effectiveness of our tool flow, we presented the mapping of a IEEE 802.11b transmitter SDR implementation to our architecture and optimized the system in terms of execution time and energy consumption by introducing instruction set extensions and dedicated hardware accelerators. These hardware extensions achieve a speed up by a factor of ten and reduce energy by about 91 %.

Acknowledge

Substantial parts of the research described in this paper were funded by the Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung – BMBF) registered there under grant number 01BU0643 (Easy-C).

References

1. Bagheri, R., Mirzaei, A., Chehrazi, S., Heidari, M., Lee, M., Mikhemar, M., Tang, W., Abidi, A.: An 800MHz to 5GHz software-defined radio receiver in 90nm CMOS. ISSCC Dig. Tech. Papers, 480–481 (2006)
2. Bluethgen, H.M., Grassmann, C., Raab, W., Ramacher, U., Hausner, J.: A programmable baseband platform for software-defined radio. In: Proceedings of SDR FORUM (2004)
3. Dreesen, R., Jungeblut, T., Thies, M., Porrmann, M., Kastens, U., Rückert, U.: A Synchronization Method for Register Traces of Pipelined Processors. In: Analysis, Architectures and Modelling of Embedded Systems, pp. 207–217. Springer, Boston (2009)
4. Halfhill, T.R.: Intel maps wireless future. Microprocessor Report 23, 1–4 (2003)
5. Jungeblut, T., Dreesen, R., Porrmann, M., Rückert, U., Hachmann, U.: Design Space Exploration for Resource Efficient VLIW-Processors. In: University Booth of the Design, Automation and Test in Europe (DATE) Conference (2008)

6. Kastens, U., Le, D.K., Slowik, A., Thies, M.: Feedback driven instruction-set extension. In: Proceedings of ACM SIGPLAN/SIGBED 2004 Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES 2004), Washington, D.C., USA (June 2004)
7. Mitola, J.: The software radio architecture. IEEE Communications Magazine 33(5), 26–38 (1995)
8. Mitola III., J.: Software radios: Survey, critical evaluation and future directions. IEEE Aerospace and Electronic Systems Magazine 8(4), 25–36 (1993)
9. Porrmann, M., Hagemeyer, J., Romoth, J., Strugholtz, M.: Rapid Prototyping of Next-Generation Multiprocessor SoCs. In: Proceedings of Semiconductor Conference Dresden, SCD 2009, Dresden, Germany, pp. 29–30 (2009)
10. Shiba, H., Shono, T., Shirato, Y., Toyoda, I., Uehara, K., Umehira, M.: Software defined radio prototype for PHS and IEEE 802.11 wireless LAN. IEICE Transactions On Communications E Series B 85(12), 2694–2702 (2002)
11. Shono, T., Shirato, Y., Shiba, H., Uehara, K., Araki, K., Umehira, M.: IEEE 802.11 wireless LAN implemented on software defined radio with hybrid programmable architecture. IEEE Transactions on Wireless Communications 4(5), 2299–2308 (2005)

On the Maximum Efficiency of Power Amplifiers in OFDM Broadcast Systems with Envelope Following

Robert Wolf*, Frank Ellinger, and Ralf Eickhoff**

Technische Universität Dresden, Chair for Circuit Design and Network Theory

Abstract. We suggest a method for determining the efficiency of the power amplifier of an OFDM broadcast system. We present how far the efficiency of conventional power amplifiers can be increased by applying envelope following. The dependency of the efficiency on the probability of clipping is derived. In this context all three possibilities of operating point adjustment are investigated. Finally, we show that by adjusting only the operating point voltage of the power amplifier the efficiency of OFDM broadcast systems can be doubled.

Keywords: OFDM, envelope following, power amplifier, efficiency, broadcast, DVB-T, operating point adjustment.

1 Introduction

The energy required for communication and its price is increasing further and further. In the meanwhile the costs for the energy used by a base station for wireless communication are higher than the investment costs [1,2]. Thus, energy efficiency of communication systems is an important topic on the one hand for the conservation of the environment and on the other hand to reduce costs.

The power amplifier of a wireless communication system contributes significantly to the power consumption. Thus, a highly efficient power amplifier is required for an efficient communication system. Unfortunately, there are several reasons why the efficiency of the power amplifier is lower than intended. Firstly, modern and future wireless communication standards, e.g., DVB-T (Digital Video Broadcasting — Terrestrial) and LTE (Long Term Evolution), require highly linear power amplifiers to obtain their high spectral efficiency. Thus, class A or class AB power amplifiers are typically applied despite their lower maximum efficiency in comparison to the more efficient switched mode power amplifiers. And secondly, those power amplifiers are typically operated in back-off. Back-off is defined as the ratio between maximum output power $P_{\mathrm{out,max}}$

---

[*] This work is partly funded by the Federal Ministry of Education and Research (BMBF) in the excellence cluster *Cool Silicon*, project *Cool Broadcast Repeater*.

[**] This work is partly funded by the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n°213952 (MIMAX).

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 160–170, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

and instantaneous output power P_{out}. If a power amplifier is operated in back-off the instantaneous output power is lower than the maximum output power. The efficiency of a class A power amplifier is proportional to the output power and is maximal at the maximum output power. Taking this into account it becomes clear that the efficiency in operation is noticeably lower than the already low maximum efficiency of the class A power amplifier. The first reason for the limited efficiency is a systematic one and has to be accepted. But concerning the second reason it is possible to increase the efficiency of a class A power amplifier in back-off by operating point adjustment.

Operating point adjustment has already been used to lessen the drop in efficiency caused by slow changes of the required output power. Such changes can be caused by altering channel conditions. If the channel changes, e.g., if a UMTS (Universal Mobile Telecommunications System) mobile phone gets closer to its base station, the output power has to be reduced to keep the received power constant. This is especially for code division multiple access (CDMA) systems like UMTS necessary but also other communication standards demand a control of the received power. The information about the required output power can be used by the baseband module to control the operating point of the power amplifier. This method is called envelope tracking. Since the changes are slow and the bandwidth is small it is relatively simple to implement an efficient operating point adjustment system. The gain in efficiency can easily be calculated by means of the statistic description of the output power. Figure 1 shows the probability density function of the output power for an UMTS device.

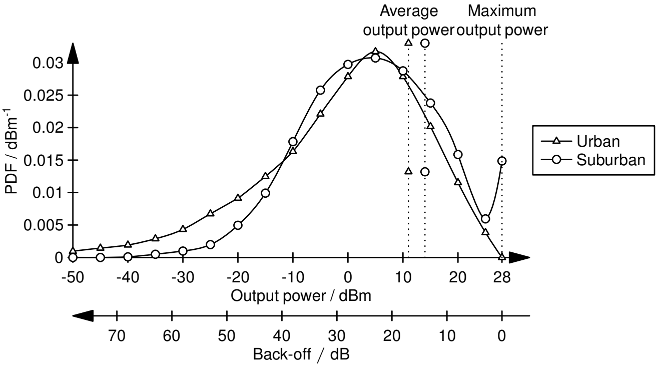


Fig. 1. Probability density function of the output power for an UMTS device [3,4]

Envelope tracking does not take into account the back-off operation caused by the modulation. Furthermore, it cannot be applied for all systems because a feedback about the channel conditions is required and an additional interface between the baseband module and the power amplifier has to be implemented. The envelope following method does not have these drawbacks. In this case the required output power is directly sensed at the power amplifier and the operating point is adjusted in real-time. Thus, the changes of the output power caused by the modulation can be exploited. Thereby, even the efficiency of broadcast systems can be increased. The power amplifier together with the operating point control becomes a stand-alone system, which makes it simple to upgrade existing systems.

In order to investigate the effect of the modulation on the efficiency and how far this influence can be lessen by envelope following, an orthogonal frequency-division multiplex (OFDM) broadcast system like DVB-T is assumed in the further course.

2 System Model

Figure 2 shows a model of the RF front-end applying envelope following. The signals I and Q modulate the carrier and the orthogonal carrier, respectively, which up-converts the spectrum into the radio frequency (RF) domain. The envelope of the RF signal is sensed and forms the reference of the operating point control which adjusts and controls the operating point of the power amplifier accordingly.

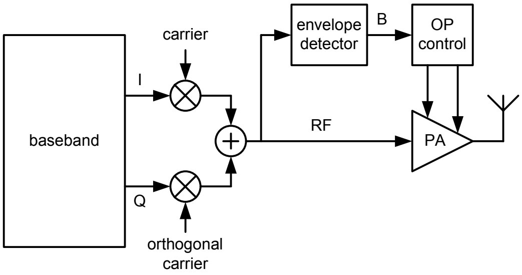


Fig. 2. Model of the transmitter of an OFDM system using envelope following as operating point control method

The envelope detector down-converts the RF signal such that the signal B corresponds to a baseband signal. Thus, an equivalent complex baseband model can be used, which is shown in figure 3. Therein, the envelope detector is replaced by its corresponding mathematical operation, which is

$$B = \sqrt{P} = \sqrt{I^2 + Q^2}. \qquad (1)$$

In order to be able to calculate the efficiency, all signals will be regarded as stochastic processes in the further course. The following assumptions and simplifications have to be made to be able to specify properties of the stochastic processes. Figure 4 depicts a block diagram of the baseband module of an OFDM transmitter including important components like the inverse discrete

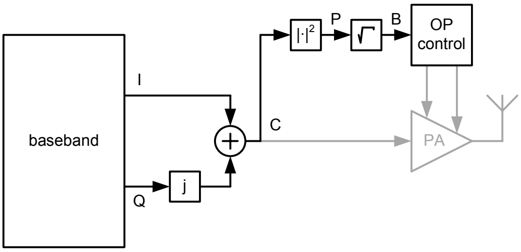


Fig. 3. Equivalent complex baseband model of the transmitter

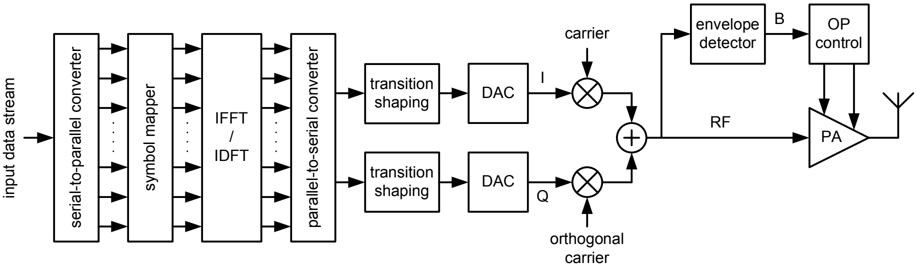


Fig. 4. Block diagram of the baseband module of an OFDM transmitter

fourier transform (IDFT) block and blocks to shape the transitions from one symbol to the next. It is assumed that the impact of those shaping blocks on the signal properties is negligible. This assumption bases on the fact that in a typical OFDM system the signal is modified by the shaping blocks just for a small fraction of time in comparison to the duration of the symbol itself.

3 Signal Properties

In a first step the properties of the processes I and Q will be derived. For OFDM systems it is often assumed that those processes are normally distributed [5,6]. This is a plausible assumption: The signals on the subcarriers can be assumed to be identically distributed processes and with the central limit theorem the superposition of many independent and identically distributed processes results in a normally distributed process.

Each normal distribution is characterized by its expected value μ and its standard deviation σ. Since each subcarrier is zero-mean, the superposition of all subcarriers is also zero-mean. The standard deviation can be determined by using the fact that the sum of the average power of all subcarriers is equal to the average power of the superposition. Thus, we are now looking for the average power $P_{\text{mean,sub}}$ of one modulated subcarrier. Figure 5 exemplarily shows the constellation diagram of a QAM16 modulation. In this case there are four

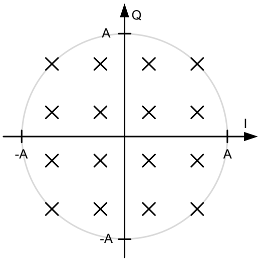


Fig. 5. Constellation diagram of the QAM16 modulation

possible amplitudes a_i for the real and for the imaginary part of the subcarrier. Assuming that each level has the same probability the average power of one modulated subcarrier can be calculated by

$$P_{\mathrm{mean,sub}} = \frac{1}{n}\sum_{i=1}^{n} a_i^2, \tag{2}$$

where n is the number of possible amplitudes. In case of the QAM16 modulation the average power is $\frac{5}{18}A^2$. The average power of one modulated subcarrier can also be calculated using the peak-to-average power ratio of the modulation. The peak-to-average power ratio $PAPR$ is defined by

$$PAPR = \frac{P_{\mathrm{peak}}}{P_{\mathrm{mean}}} = \frac{V_{\mathrm{peak}}^2}{V_{\mathrm{rms}}^2} = CF^2 \tag{3}$$

where P_{peak}, P_{mean}, and CF are the peak power, the mean power, and the crest factor of a signal, respectively. Following this definition the peak-to-average power ratio of the QAM16 modulation is

$$PAPR_{\mathrm{mod,QAM16}} = \frac{\left(1\right)^2}{\frac{4}{16}\cdot\left(1\right)^2 + \frac{8}{16}\cdot\left(\frac{\sqrt{5}}{3}\right)^2 + \frac{4}{16}\cdot\left(\frac{1}{3}\right)^2} = \frac{9}{5}. \tag{4}$$

The peak-to-average power ratios of some other modulations are listed in table 1.

Using the peak-to-average power ratio for the calculation the average power can be determined by

$$P_{\mathrm{mean,sub}} = \frac{P_{\mathrm{peak,sub}}}{PAPR_{\mathrm{mod}}} = \frac{\left(\frac{A}{\sqrt{2}}\right)^2}{PAPR_{\mathrm{mod}}}. \tag{5}$$

Table 1. Peak-to-average power ratios of some modulation schemes

Modulation	QPSK	QAM16	QAM64	QAM256	QAMn^2
$PAPR_{\mathrm{mod}}$	1	$\frac{9}{5}$	$\frac{7}{3}$	$\frac{45}{17}$	$\frac{3(n-1)}{n+1}$
	0 dB	2.6 dB	3.7 dB	4.2 dB	

Now the average power of the processes I and Q can be specified to be

$$P_{\mathrm{mean,I/Q}} = n_{\mathrm{sub}}\ P_{\mathrm{mean,sub}} = \tfrac{1}{2} n_{\mathrm{sub}} \frac{A^2}{PAPR_{\mathrm{mod}}}. \tag{6}$$

Since the processes I and Q are zero-mean, the variance σ^2 is equal to the average power. Thus the standard deviation σ can be calculated by

$$\sigma = \sqrt{P_{\mathrm{mean,I/Q}}} = \sqrt{\tfrac{1}{2} n_{\mathrm{sub}} \frac{A^2}{PAPR_{\mathrm{mod}}}} \tag{7}$$

and the probability density function is finally given by

$$p_{\mathrm{I/Q}}(x) = \tfrac{1}{\sqrt{2\pi}\sigma}\ e^{-\frac{x^2}{2\sigma^2}}. \tag{8}$$

In addition the peak-to-average power ratio of the processes I and Q can be specified to be

$$\begin{aligned} PAPR_{\mathrm{I/Q}} &= \frac{P_{\mathrm{peak,I/Q}}}{P_{\mathrm{mean,I/Q}}} \quad \text{with} \quad P_{\mathrm{peak,I/Q}} = \left(n_{\mathrm{sub}} \frac{A}{\sqrt{2}} \right)^2 \\ &= n_{\mathrm{sub}}\ PAPR_{\mathrm{mod}}. \end{aligned} \tag{9}$$

This shows the fundamental disadvantage of OFDM systems: the peak-to-average power ratio and the crest factor increase with the number of subcarriers and with the square root of the number of subcarriers, respectively.

According to (1) the process P is characterized by $P = I^2 + Q^2$. This implies the the process P is Chi-square distribution [7] with the probability density function

$$p_P(x) = \begin{cases} \frac{1}{2\sigma^2}\ e^{-\frac{x}{2\sigma^2}} & x \geq 0 \\ 0 & x < 0 \end{cases}. \tag{10}$$

This is identical to the probability density function of an exponential distribution. By applying the density transformation the probability density function of the process B can be derived:

$$p_B(x) = \begin{cases} \frac{x}{\sigma^2}\ e^{-\frac{x^2}{2\sigma^2}} & x \geq 0 \\ 0 & x < 0 \end{cases}. \tag{11}$$

This is a special case of the Weibull distribution and also called Rayleigh distribution.

4 Dependency of the Efficiency on the Drive

We already discussed that the operating point of the power amplifier can be adjusted and that thereby the efficiency can be enhanced. In this section the

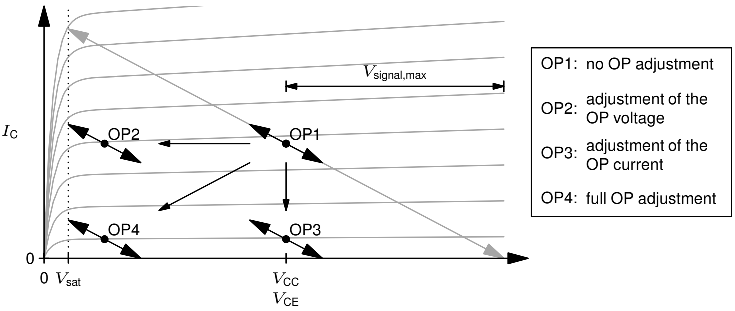


Fig. 6. The different possibilities of the OP adjustment visualized in the output characteristics of a transistor

relation between efficiency and the drive of the power amplifier for the different possibilities of operating point adjustment is derived.

The two main operating point (OP) parameters of a transistor and thereby of the power amplifier are OP voltage and OP current. The OP can be visualized in the output characteristics of the transistor together with the load line. The power amplifier operates linearly as long as the current in the transistor is greater than zero and the voltage across the transistor is greater than the saturation voltage [8]. The maximum drive is illustrated in figure 6 by the gray arrow. In this case the power amplifier delivers its maximum output power. It can be seen that if less output power is needed and thereby the swing is smaller the limitations for linear operation are not reached. This means that the OP is chosen to high for this particular output power and energy is wasted. Thus, one or both OP parameters can be adjusted such that the respective OP parameter(s) are minimized subject to the restrictions mentioned above. This is depicted in figure 6 by means of the three additional operating points (OP2, OP3, and OP4). That way the efficiency can be calculated for each case by means of the power taken from the supply and the power delivered to the load, which is always

$$P_{\mathrm{out}} = \frac{V_{\mathrm{signal}}^2}{2R_{\mathrm{load}}}. \tag{12}$$

For the case that the OP is not adjusted, the power P_{DC} taken from the supply is independent from the signal and is

$$P_{\mathrm{DC}} = V_{\mathrm{CC}}\, I_{\mathrm{C,OP}} = (V_{\mathrm{signal,max}} + V_{\mathrm{sat}})\, \frac{V_{\mathrm{signal,max}}}{R_{\mathrm{load}}}. \tag{13}$$

The efficiency is given by

$$\eta_{\mathrm{no}} = \frac{P_{\mathrm{out}}}{P_{\mathrm{DC}}} = \tfrac{1}{2}\,\frac{(V_{\mathrm{signal}}/V_{\mathrm{signal,max}})^2}{1 + V_{\mathrm{sat}}/V_{\mathrm{signal,max}}}. \tag{14}$$

This equation shows that the maximum efficiency η_{max} of a class A amplifier is 50% which can theoretically be achieved if the saturation voltage is set to zero.

For the deviation of this equation it was assumed that the resistance of the load line is equal to the resistance of the connected load. This implies for instance an infinite output resistance of the transistor. Since this is practically not the case the parameter $\eta_{\max}$ is introduced to take aditional losses into account. Thus, the efficiency in this case and for all the other cases can be determined to be

$$\text{OP1:} \quad \eta_{\text{no}} = \eta_{\max} \frac{(V_{\text{signal}}/V_{\text{signal,max}})^2}{1 + V_{\text{sat}}/V_{\text{signal,max}}} \tag{15}$$

$$\text{OP2:} \quad \eta_{\text{V}} = \eta_{\max} \frac{V_{\text{signal}}/V_{\text{signal,max}}}{1 + V_{\text{sat}}/V_{\text{signal}}} \tag{16}$$

$$\text{OP3:} \quad \eta_{\text{C}} = \eta_{\max} \frac{V_{\text{signal}}/V_{\text{signal,max}}}{1 + V_{\text{sat}}/V_{\text{signal,max}}} \tag{17}$$

$$\text{OP4:} \quad \eta_{\text{VC}} = \eta_{\max} \frac{1}{1 + V_{\text{sat}}/V_{\text{signal}}} . \tag{18}$$

In order to understand the impact of the saturation voltage Figure 7 illustrates these functions in a simplified way. Thereby, the curve for no OP adjustment shows the typically back-off behaviour of a class A power amplifier whose efficiency is proportional to the output power. If either the OP current or the OP voltage are adjusted it can be seen that the drop in efficiency can be reduced. In case that the OP voltage and the OP current are adapted the efficiency is almost kept constant till the losses caused by the saturation voltage are significant in comparison to the output power.

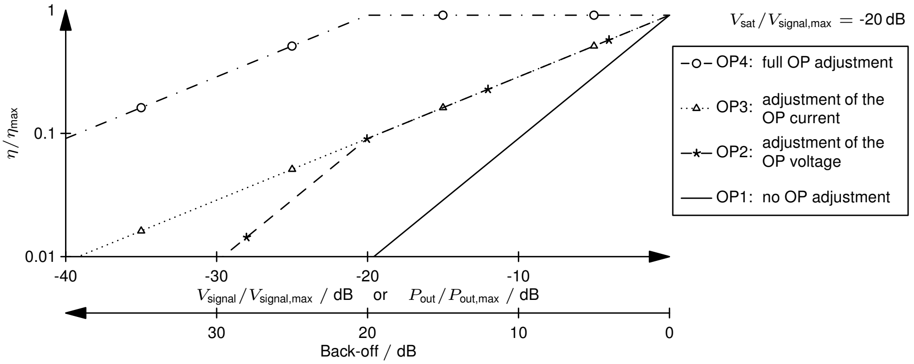


Fig. 7. Simplified dependency of the normalized efficiency versus the normalized output power for the different possibilities of the OP adjustment

5 Efficiency of the System

The average efficiency of the system can be determined by using the derived properties of the stochastic process in combination with the derived formulas for the efficiency. In order to do so it have to be considered that it is practically not possible to design an OFDM system that the full dynamic range of the signal, which is described by the crest factor, is in the range of linear operation. Thus, depending on the systems there is a certain probability of clipping. Clipping means that more output power and more signal swing is demanded from the power amplifier than its maximum output power and maximum signal swing, respectively. The probability of clipping can be influenced by the ratio between maximum output power of the power amplifier and its average output power.

The maximum voltage swing $V_{\mathrm{signal,max}}$ at the output of the power amplifier is set by given constraints like breakdown and saturation voltage. For a desired probability of clipping a proper value for the parameter σ of the Rayleigh distributed voltage envelope of the signal has to be chosen (cf. figure 8). This influences the mean voltage of the signal. In order to achieve the required mean output power the OP current and the load line have to be adapted. Raising the OP current for a given OP voltage is equivalent to increasing the maximum output power of the power amplifier.

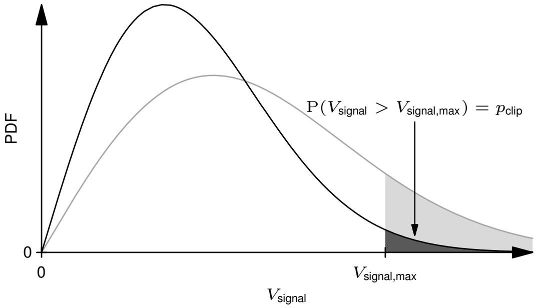


Fig. 8. Influence of the parameter of the Rayleigh distribution on the probability density function of the voltage envelope for a high (gray) and a low (black) probability of clipping, respectively for low and a high ratio between maximum and average output power

The resulting average efficiency versus the probability of clipping can be determined. Thereto, the probability density function of the signal envelope has to be transformed using the relationship between the amplitude and the efficiency derived above to get the probability density function of the efficiency. Afterwards, the average value of the efficiency can be evaluated making use of the transformed density function. The result is depicted in figure 9. The improvement in comparison to a system without operating point adjustment is illustrated in figure 10.

Regarding the clipping probability there are two extreme cases. The first is the operation with 100% clipping, which theoretically is the most efficient because the power amplifier always operates in saturation. Thus, OP adjustment has no benefit, which can be seen in figure 9 where all curves converge to one point. Furthermore, this is not practically relevant because the signal is completly

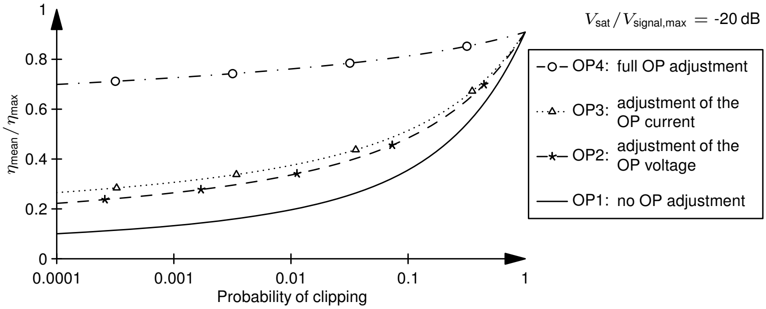


Fig. 9. Average efficiency versus the probability of clipping

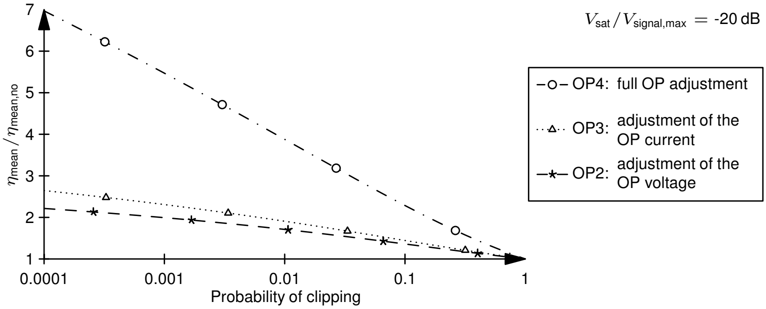


Fig. 10. Benefit of the OP adjustment versus the probability of clipping

distorted which results in a bit error ratio of 0.5. The other extreme case is an operation with almost no clipping, i.e., a very low bit error ratio. In this case the efficiency drops significantly for all kinds of operating point adjustment. For the design of a practical system there is a trade-off between efficiency and bit error ratio.

The designer of a power amplifier needs to know the required maximum output power $P_{\mathrm{out,max}}$. This value can be derived by using the average output power $P_{\mathrm{out,mean}}$ and the probability of clipping p_{clip} which are set by the system designer. Since the power of the signal is exponentially distributed, which was derived in section 3, the probability of clipping is

$$\begin{aligned} p_{\mathrm{clip}} &= \mathrm{P}\left(P_{\mathrm{out,mean}} > P_{\mathrm{out,max}}\right) \\ &= e^{-\frac{P_{\mathrm{out,max}}}{P_{\mathrm{out,mean}}}} = e^{-PAPR_{\mathrm{PA}}} \end{aligned} \tag{19}$$

which can be rearranged to

$$PAPR_{\mathrm{PA}} = -\ln\left(p_{\mathrm{clip}}\right) . \tag{20}$$

For typical systems the peak-to-average power ratio $PAPR_{\mathrm{PA}}$, for which the power amplifier is designed, is about 7 dB which is relatively low in comparison to the peak-to-average power ratio of a DVB-T signal of approximately 35 dB an which results in a probability of clipping of around 0.7%.

Due to several drawbacks the adjustment of the OP current is rather difficult. Thus, adjusting only the OP voltage in combination with envelope following is often applied [9]. Even for this case it can be seen that the efficiency of OFDM broadcast systems can be increased by a factor of two.

6 Conclusion

We theoretically analyzed the maximum efficiency of the power amplifier of an OFDM broadcast system with envelope following. Thereto, we investigated the efficiency of OFDM system without operating point adaption, with OP voltage, with operating point current, and with full operating point adjustment. We showed that adapting the operating point is beneficial even for broadcast systems. Thereby, a gain in efficiency by the factor of two for the modulation of a single operating point parameter and a factor of four for the modulation of both operating point parameters can be achieved. Since the calculated relations based on idealized models the gain in efficiency might be lower in practical implementations. Additionally, we showed that there is a trade-off between efficiency and signal quality by means of the probability of clipping and we depicted how the requirements on the power amplifiers are related to the system parameters.

The derivations were done having a broadcast system in mind. But all considerations can also be applied for bidirectional wireless communication systems. Therefore, the results of the statistic investigations on the output power level for the particular standard, which was illustrated for UMTS in figure 1, have to be taken additionally into account.

References

1. Fettweis, G.P., Ellinger, F. et al.: Cool Silicon. In: Congress Cool Silicon (2009)
2. Fettweis, G.P., Zimmermann, E.: ICT energy consumption - trends and challenges. In: 11th International Symposium on Wireless Personal Multimedia Communications (2008)
3. CDMA Development Group: CDG Stage 4 System Performance Tests (1998)
4. Groe, J.B., Larson, L.E.: CDMA Mobile Radio Design, 1st edn. Artech House, Norwood (2000), ISBN 1–58053–059–1
5. Eltholth, A.: Low Crest Factor Modulation Techniques for Orthogonal Frequency Division Multiplexing (OFDM). In: UbiCC, vol. 2(5) (2007)
6. Rhode, Schwarz: Der Crest-Faktor bei DVB-T-(OFDM-)Sendeanlagen und seine Auswirkung auf die Dimensionierung der Leistungskomponenten, – Application Note 7TS02 (2007)
7. Proakis, J.G.: Digital Communications, 4th edn. McGraw-Hill, New York (2000), ISBN 0–07–232111–3
8. Cripps, S.C.: RF Power Amplifiers for Wireless Communications, 2nd edn. Artech House, Norwood (2006), ISBN 1–59693–018–7
9. Haßler, F., Ellinger, F., Carls, J.: Analysis of buck-converters for efficiency enhancements in power amplifiers for wireless communication. In: IEEE Microwave and Optoelectronics Conference, pp. 616–620 (2007)

Equal-Phase Beamforming Architecture for RF-MIMO Antenna Systems

Fouad Gholam, Javier Vía, Alfredo Nazábal, and Ignacio Santamaría

Communications Engineering Department (DICOM)
University of Cantabria, Santander, 39005, Spain
{fouad,jvia,alfredo,nacho}@gtas.dicom.unican.es

Abstract. This paper considers a novel multiple-input multiple-output (MIMO) architecture, which combines the signals in the radio-frequency (RF) domain. Unlike previous approaches, the proposed architecture is exclusively based on the application of different gain factors to the transmitted/received signals, and therefore it avoids the need of including a controllable phase-shifter (or sign switch) for each transmit/receive antenna. From a baseband point of view, the transceiver design consists in obtaining the optimal equal phase transmit (EPT) and equal-phase combining (EPC) beamformers. Interestingly, this problem can be exactly solved in the case of rank-one channels, which can be exploited to construct an iterative algorithm for the general MIMO case. The proposed architecture is evaluated by means of Monte Carlo simulations, which show that the slight performance degradation with respect to previous approaches is justified by the significant reduction in the hardware cost and power consumption.

Keywords: RF-MIMO beamformer, equal-phase MIMO beamforming, semidefinite relaxation (SDR).

1 Introduction

One of the most important problems for the commercial deployment of new generation multiple-input multiple-output (MIMO) systems consists in the high hardware complexity and power consumption associated to conventional MIMO transceivers. This high costs are due to the need of replicating the up/down conversion RF chains for each transmit and receive antenna. In order to alleviate this drawback, several alternative architectures have been proposed in the last years. These solutions range from the idea of pre-FFT combining systems [4–6], which reduces the number of FFT blocks in multicarrier systems (but still requires the replication of the RF chains), to truly analog antenna combining systems [1, 7–10], which combine the signals in the RF domain and only require one RF chain.

In this paper we consider a new simplification of RF-MIMO transceivers. In particular, we show that the hardware complexity can be significantly reduced by removing the controllable phase shifters (or sign switch modules) required in previously proposed architectures. Obviously, the simplification of the RF hardware comes at a cost of a slightly reduced performance. However, we will show that, by properly selecting the amplification factors in each RF branch, the performance of this alternative architecture is close to that of previous approaches.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 171–179, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

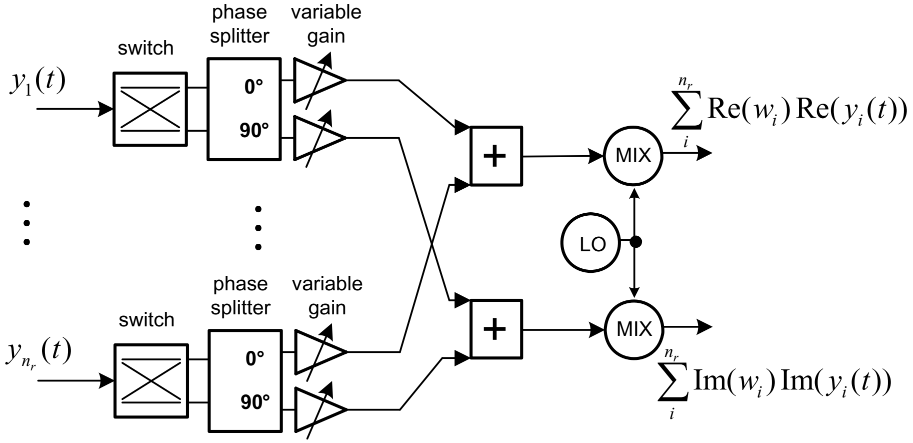


Fig. 1. RF-MIMO Architecture. Original design including variable gain amplifiers and phase shifters.

From a baseband point of view, the transceiver design consists in selecting the optimal amplification factors for each antenna. In other words, the proposed architecture forces us to work with equal phase transmit (EPT) and equal phase combining (EPC) beamformers, which are defined by the amplification factors. In the case of rank-one MIMO channels, which include the cases of single-input multiple-output (SIMO) and multiple-input single-output (MISO) systems, the optimal beamformer can be obtained by means of a semidefinite relaxation (SDR) approach [2]. Thus, in order to solve the general MIMO EPT/EPC beamforming problem, we propose an iterative algorithm consisting in alternating the optimization of the transmit and receive beamformers. Finally, the performance of the proposed architecture and algorithm is illustrated by means of some Monte Carlo simulations, which show that the slight performance degradation is justified by the significant decrease in the hardware complexity and power consumption.

2 RF-MIMO Architectures

In order to reduce the hardware cost and power consumption associated to conventional MIMO transceivers, some recent works have considered the possibility of moving part of the signal processing from the baseband to the RF domain [1, 7–10]. Specifically, Fig. 1 shows an analog antenna combining system, which avoids the replication of the up (or down) conversion chains for all the transmit/receive antennas. Thus, the transmitted/received signals can be weighted (complex weights) and combined in the RF domain, which results in a simplified architecture with a performance close to that of conventional MIMO systems [7, 10].

In order to further simplify the original RF-MIMO architecture, in [3] we have proposed a system based on the application of a real gain factor to each signal (see Fig.

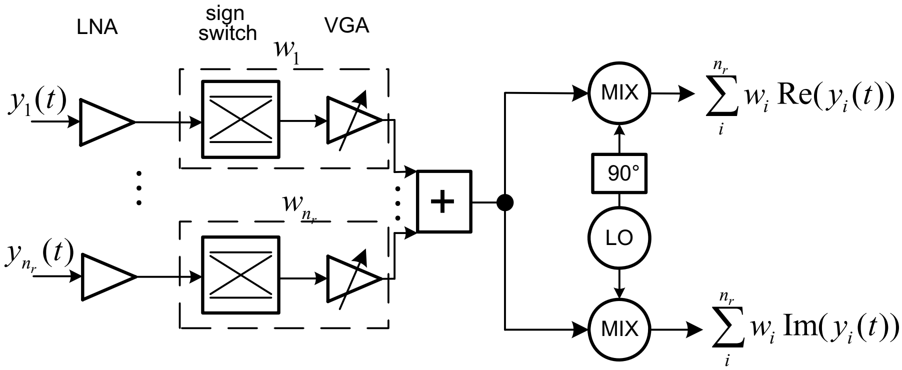

LNA
sign switch
VGA
w_1
w_{n_r}
$y_1(t)$
$y_{n_r}(t)$
+
MIX
90°
LO
MIX
$\sum_i^{n_r} w_i \,\mathrm{Re}(y_i(t))$
$\sum_i^{n_r} w_i \,\mathrm{Im}(y_i(t))$

Fig. 2. Simplified RF-MIMO Architecture. The phase shifters are replaced by sign-switch modules, which translates into beamformers with real coefficients.

2), which introduces the constraint of applying beamformers with real coefficients (RF weights). In this work we propose an additional simplification, which allows us to remove the sign-switch blocks in Fig. 2, and introduces the additional constraint of having equal-phase transmit (EPT) and equal-phase combining (EPC) beamformers. The proposed RF-MIMO architecture is illustrated in Fig. 3, and in this work we consider the problem of designing the transmit and receive beamformers under the assumption of perfectly known flat-fading and static[1] MIMO channels.

3 Design of the Beamformers

Throughout this paper we will use bold-faced upper case letters to denote matrices, bold-faced lower case letters for column vector, and light-faced lower case letters for scalar quantities. Superscripts $(\cdot)^T$ and $(\cdot)^H$ denote transpose and Hermitian respectively. $\|\mathbf{A}\|$, $\mathrm{Tr}(\mathbf{A})$, $\mathrm{rank}(\mathbf{A})$ and $\mathrm{vec}(\mathbf{A})$ will denote, respectively, the Frobenius norm, trace, rank, and column-wise vectorized version of matrix $\mathbf{A}$. $\mathrm{unvec}(\mathbf{a})$ is the inverse of the $\mathrm{vec}(\mathbf{A})$ operation, i.e., $\mathrm{unvec}(\mathrm{vec}(\mathbf{A})) = \mathbf{A}$. $\mathbf{A} \succeq \mathbf{0}$ means that $\mathbf{A}$ is symmetric and positive semidefinite, whereas $\mathbf{A} \geq \mathbf{0}$ means that the elements of $\mathbf{A}$ are non-negative. $\Re(\mathbf{A})$ denotes the real part of the complex matrix $\mathbf{A}$, and $\mathbf{u}_{\max}(\mathbf{A})$ is the principal eigenvector of the positive semidefinite matrix $\mathbf{A}$. Finally, $\mathbf{I}$ and $\mathbf{0}$ are the identity and zero matrices of the required dimensions.

Assuming n_T transmit and n_R receive antennas, the data model after Tx-Rx beamforming can be written as

$$y = hs + n,$$

---

[1] In the case of time-varying channels, the design of the beamformers would follow the same lines. However, the channel estimation process for the simplified architectures requires more training time than in the conventional MIMO case.

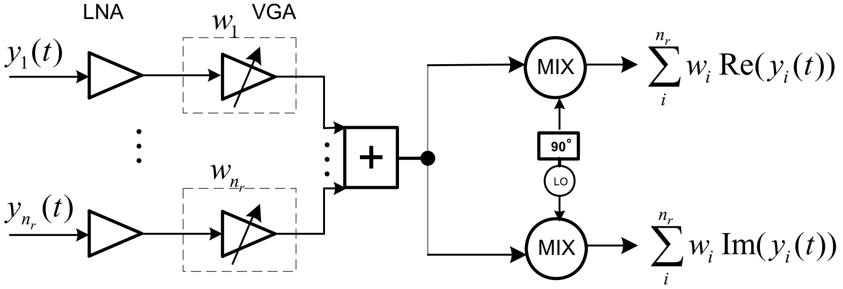

LNA
w_1
VGA
$y_1(t)$
w_{n_r}
$y_{n_r}(t)$
+
MIX
90°
LO
MIX
$\sum_i^{n_r} w_i \operatorname{Re}(y_i(t))$
$\sum_i^{n_r} w_i \operatorname{Im}(y_i(t))$

Fig. 3. Proposed simplification of the RF-MIMO Architecture. The phase shifters and sign-switch modules are avoided, which comes at the price of working with equal phase transmit (EPT) and equal phase combining (EPC) beamformers.

where $s \in \mathbb{C}$ represents the transmitted signal (information symbols), $y \in \mathbb{C}$ is the observation, $n \in \mathbb{C}$ represents the noise,

$$h = \mathbf{w}_R^T \mathbf{H} \mathbf{w}_T,$$

is the equivalent channel after Tx-Rx beamforming, $\mathbf{H} \in \mathbb{C}^{n_R \times n_T}$ is the MIMO channel, and $\mathbf{w}_T \in \mathbb{R}^{n_T \times 1}$, $\mathbf{w}_R \in \mathbb{R}^{n_R \times 1}$ represent the transmit and receive beamformers, which are defined by the gain factors applied to each antenna. Thus, the optimization problem associated to the design of the beamformers can be written as

$$\begin{aligned} \underset{\mathbf{w}_T, \mathbf{w}_R}{\text{maximize}} \quad & |\mathbf{w}_R^T \mathbf{H} \mathbf{w}_T| \\ \text{subject to} \quad & \|\mathbf{w}_T\| \le 1, \\ & \|\mathbf{w}_R\| \le 1, \\ & \mathbf{w}_T \ge \mathbf{0}, \\ & \mathbf{w}_R \ge \mathbf{0}, \end{aligned} \tag{1}$$

where we can readily identify the conventional energy constraints, as well as the additional positiveness constraints due to the removal of the sign-switch blocks.

3.1 Beamformer Design in the SIMO and MISO Cases

Unfortunately, the optimization problem in (1) is not convex, which precludes its solution by means of standard convex optimization tools [2]. However, in the case of rank-one channels (which includes the SIMO and MISO cases), the optimal solution of (1) can be obtained by means of a semidefinite relaxation (SDR) approach [2].

Let us consider the SIMO case[2] and write the optimization problem in (1) as

$$\begin{aligned} \underset{\mathbf{w}_R}{\text{maximize}} \quad & \mathbf{w}_R^T \mathbf{R} \mathbf{w}_R \\ \text{subject to} \quad & \|\mathbf{w}_R\| \le 1, \\ & \mathbf{w}_R \ge \mathbf{0}, \end{aligned}$$

---

[2] The analysis for the MISO case (or the more general case of rank-one MIMO channels) can be made in a similar manner.

where

$$\mathbf{R} = \Re(\mathbf{h}\mathbf{h}^H),$$

and $\mathbf{h} \in \mathbb{C}^{n_R \times 1}$ is the the SIMO channel.

Defining now the beamforming matrix $\mathbf{W}_R = \mathbf{w}_R \mathbf{w}_R^T$, it is easy to see that the above optimization problem can be rewritten as

$$\begin{aligned} \underset{\mathbf{W}_R}{\text{maximize}} \quad & \text{Tr}(\mathbf{R}\mathbf{W}_R) \\ \text{subject to} \quad & \text{Tr}(\mathbf{W}_R) \leq 1, \\ & \mathbf{W}_R \geq \mathbf{0}, \\ & \mathbf{W}_R \succeq \mathbf{0}, \\ & \text{rank}(\mathbf{W}_R) = 1, \end{aligned} \tag{2}$$

where, excluding the rank-one constraint, we have three convex constraints and a concave objective function. Therefore, dropping the non-convex rank-one constraint, we obtain the following convex optimization problem

$$\begin{aligned} \underset{\mathbf{W}_R}{\text{maximize}} \quad & \text{Tr}(\mathbf{R}\mathbf{W}_R) \\ \text{subject to} \quad & \text{Tr}(\mathbf{W}_R) \leq 1, \\ & \mathbf{W}_R \geq \mathbf{0}, \\ & \mathbf{W}_R \succeq \mathbf{0}, \end{aligned} \tag{3}$$

whose solution can be obtained by means of standard convex optimization tools. More importantly, it can be proved[3] that there exists a rank-one solution for the relaxed problem in (3), or in other words, we can obtain the optimal solution of the non-convex optimization problem in (2) by solving the relaxed problem in (3).

3.2 Design of the MIMO Beamformers

In the general MIMO case, the problem of obtaining the optimal beamformers is much more complicated, and we have to resort to suboptimal approaches. Here, we propose an iterative algorithm, which is based on alternating minimizations on the transmit and receive beamformers. That is, once the transmit (respectively receive) beamformer has been fixed, the receive (resp. transmit) beamformer can be obtained as explained in the previous subsection. Thus, the overall technique is summarized in Algorithm 1, and as a convergence criterion we can use the Euclidean distance between the beamformers in two consecutive iterations. Finally, in order to guarantee the fast convergence of the algorithm, we propose an initialization approach based on a semidefinite relaxation technique.

---

[3] Although we do not provide the details here, the proof is based on the fact that there exists a rank-one matrix $\mathbf{W}_R$ satisfying the KKT conditions for the problem in (3).

```
Initialize the beamformers $\mathbf{w}_T$, $\mathbf{w}_R$.
repeat
    Update of the receive beamformer
    Obtain the equivalent SIMO channel $\mathbf{h}_{\text{SIMO}} = \mathbf{H}\mathbf{w}_T$.
    Solve the optimization problem in (2) for the SIMO channel $\mathbf{h}_{\text{SIMO}}$
    Use the obtained solution as the new receive beamformer $\mathbf{w}_R$.
    Update of the transmit beamformer
    Obtain the equivalent MISO channel $\mathbf{h}_{\text{MISO}} = \mathbf{H}^T\mathbf{w}_R$.
    Solve the optimization problem in (2) for the MISO channel $\mathbf{h}_{\text{MISO}}$
    Use the obtained solution as the new transmit beamformer $\mathbf{w}_T$.
until Convergence
```

Algorithm 1. Proposed iterative EPT-EPC beamforming algorithm

Let us start by rewriting the optimization problem in (1) as

$$\begin{array}{ll} \underset{\mathbf{w}_T,\mathbf{w}_R,\mathbf{w}}{\text{maximize}} & |\mathbf{h}^T\mathbf{w}| \\ \text{subject to} & \|\mathbf{w}_T\| \leq 1, \\ & \|\mathbf{w}_R\| \leq 1, \\ & \mathbf{w}_T \geq \mathbf{0}, \\ & \mathbf{w}_R \geq \mathbf{0}, \\ & \mathbf{w} = \mathbf{w}_T \otimes \mathbf{w}_R, \end{array}$$

where $\mathbf{h} = \text{vec}(\mathbf{H})$ is the vectorized version of the MIMO channel. Equivalently, the above problem can be rewritten as

$$\begin{array}{ll} \underset{\mathbf{w}_T,\mathbf{w}_R,\mathbf{W}}{\text{maximize}} & \text{Tr}(\mathbf{R}\mathbf{W}) \\ \text{subject to} & \text{Tr}(\mathbf{W}) \leq 1, \\ & \mathbf{W} \geq \mathbf{0}, \\ & \mathbf{W} \succeq \mathbf{0}, \\ & \text{rank}(\mathbf{W}) = 1, \\ & \mathbf{u}_{\max}(\mathbf{W}) = \mathbf{w}_T \otimes \mathbf{w}_R, \end{array} \tag{4}$$

where $\mathbf{R} = \Re(\mathbf{h}\mathbf{h}^H)$, and $\mathbf{u}_{\max}(\mathbf{W})$ denotes the principal eigenvector of matrix $\mathbf{W}$. Obviously, the above problem is not convex due to the two last constraints. However, if we relax the last constraint, we obtain the non-convex optimization problem

$$\begin{array}{ll} \underset{\mathbf{W}}{\text{maximize}} & \text{Tr}(\mathbf{R}\mathbf{W}) \\ \text{subject to} & \text{Tr}(\mathbf{W}) \leq 1, \\ & \mathbf{W} \geq \mathbf{0}, \\ & \mathbf{W} \succeq \mathbf{0}, \\ & \text{rank}(\mathbf{W}) = 1, \end{array}$$

which is identical to that in (2), and can be exactly solved by means of a SDR approach. Of course, the solution $\mathbf{W}$ of the relaxed problem does not need to satisfy the constraint $\mathbf{u}_{\max}(\mathbf{W}) = \mathbf{w}_T \otimes \mathbf{w}_R$, and therefore it is not a solution of the original problem in (4). However, we can obtain an approximated solution by first obtaining $\mathbf{w} = \mathbf{u}_{\max}(\mathbf{W})$ and forming the $n_R \times n_T$ matrix $\tilde{\mathbf{W}} = \text{unvec}(\mathbf{w})$. Thus, a good approximation to the optimal EPT and EPC beamformers can be obtained from the best (in the Euclidean-norm sense) rank-one approximation of $\tilde{\mathbf{W}}$, which is given by $\mathbf{w}_R\mathbf{w}_T^T$, where $\mathbf{w}_R$ and $\mathbf{w}_T$ are the singular vectors associated to the largest singular value of $\tilde{\mathbf{W}}$. Finally, we must note that the solution $\mathbf{W}$ satisfies the constraint $\mathbf{W} \geq \mathbf{0}$, which also implies $\mathbf{w} \geq \mathbf{0}$, $\tilde{\mathbf{W}} \geq \mathbf{0}$, and $\mathbf{w}_T \geq \mathbf{0}$, $\mathbf{w}_R \geq \mathbf{0}$, i.e., the obtained beamformers are feasible points of the original optimization problem in (1). Thus, with this initialization stage the proposed iterative EPT-EPC beamforming algorithm converges in a few iterations.

4 Simulation Results

We present below several numerical examples to demonstrate the performance of the proposed RF-MIMO architecture with EPT/EPC beamforming. In all the simulations, the transmitted signals belong to a QPSK constellation, and the flat-fading channel is generated according to an i.i.d. Rayleigh channel model. The performance is evaluated in terms of bit error rate (BER), and we have compared the following systems:

- Proposed scheme: Denoted as EPT/EPC and based on the simplified architecture shown in Fig. 3.
- Maximum ratio transmission and maximum ratio combining (denoted as MRT/MRC). This is the optimal beamforming strategy, which requires a conventional MIMO system or the RF-MIMO architecture shown in Fig. 1.
- Real beamforming (referred to as RB). This is the optimal beamforming for the simplified architecture in Fig. 2.
- Equal gain transmission and equal gain combining (EGT/EGC). This is an alternative simplification based on the use of phase shifters, and the elimination of the variable gain amplifiers.
- Selection diversity transmission and selection diversity combining (SDT/SDC). This technique consists in the selection of the best transmit/receive pair, i.e., the antennas associated to the coefficient with largest absolute value in the MIMO channel $\mathbf{H}$.

In the first simulation example we consider an scenario with only one transmit antenna. Therefore, we are obtaining the optimal receive EPC beamformer by solving the relaxed problem in (3). Fig. 4 shows the obtained results in the case of $n_R = 4$ and $n_R = 10$ receive antennas, where we can see that the proposed scheme is able to exploit all the spatial diversity in the system, and that the performance degradation with respect to more complicated RF-MIMO architectures is not greater than 3 dB.

Fig. 5 shows the results in a MIMO case with $n_T = n_R = 4$ antennas and ten iterations of the proposed iterative beamforming algorithm. Here we can see that the proposed method provides satisfactory results, and that the performance of the proposed architecture is better than that of an antenna selection method. Furthermore, we can observe that the performance of the proposed system architecture is not very far from that of other RF-MIMO systems with a higher hardware cost and power consumption.

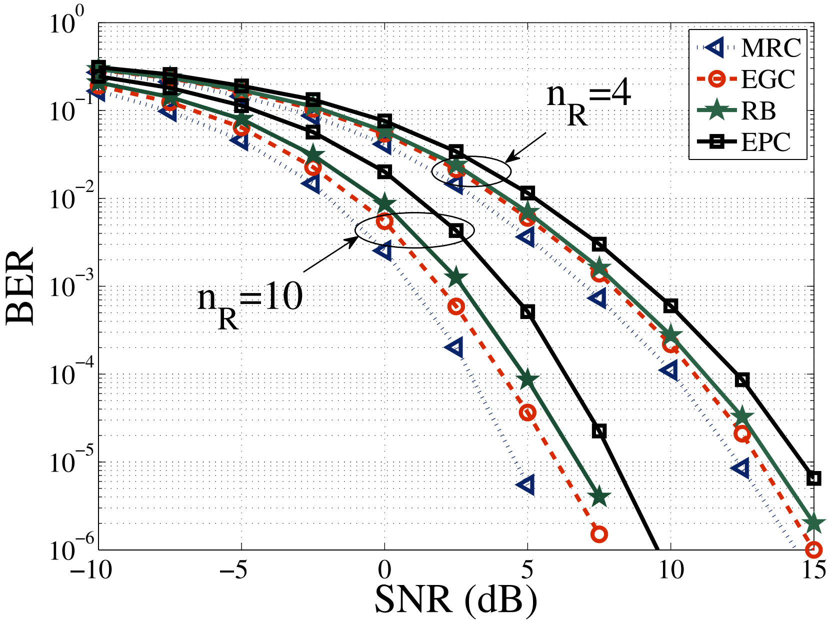


Fig. 4. Performance of the different architectures in a SIMO case

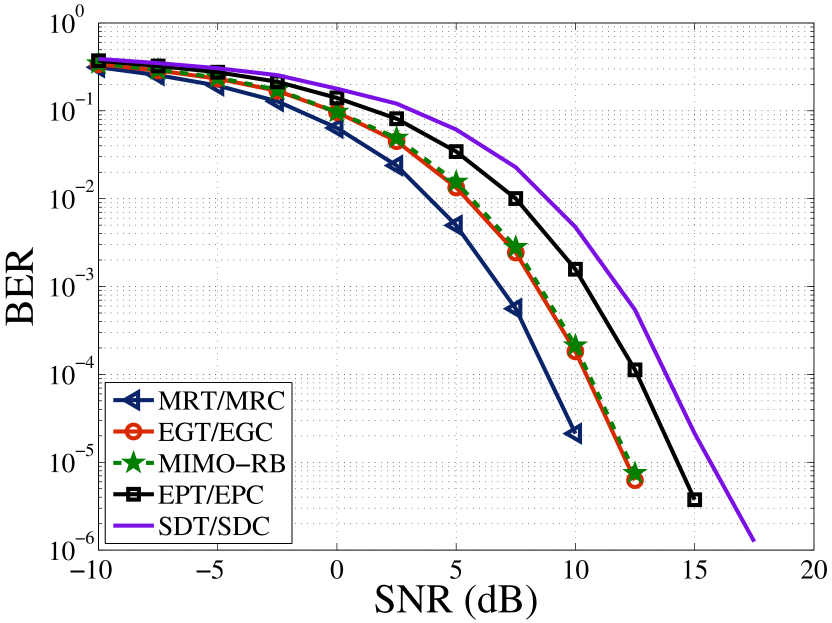


Fig. 5. Performance of the different architectures in a 4×4 MIMO case

5 Conclusion

In this paper we have presented a simplified architecture for analog antenna combining, which is based on the application of different gain factors to each RF branch. From a baseband point of view, the proposed architecture imposes the use of equal phase transmit (EPT) and equal phase combining (EPC) beamformers. In general, the design of the optimal beamformers results in a non-convex optimization problem, which can not be exactly solved by means of standard optimization techniques. However, in the case of rank-one MIMO channels, which includes the SIMO and MISO cases, the optimal beamformers can be obtained by means of a semidefinite relaxation approach. This fact is exploited to propose an iterative algorithm based on alternating optimizations of the transmit and receive beamformers. Several simulation examples illustrate the good performance of the proposed algorithm, and they also show that the significant decrease in the system cost and power consumption justifies the slight performance degradation with respect to other alternative MIMO architectures.

References

1. MIMAX: Advanced MIMO systems for maximum reliability and performance (2008), `http://www.ict-mimax.eu`
2. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press, Cambridge (2004)
3. Gholam, F., Vía, J., Santamaría, I., Wickert, M., Eickhoff, R.: Simplified architectures for analogue antenna combining. In: ICT-MobileSummit 2009, Santander, Spain (June 2009)
4. Huang, D., Letaief, K.B.: Symbol-based space diversity for coded OFDM systems. IEEE Transactions on Wireless Communications 3(1), 117–127 (2004)
5. Li, S., Huang, D., Letaief, K.B., Zhou, Z.: Pre-DFT processing for MIMO-OFDM systems with space-time-frequency coding 6(11), 4176–4182 (2007)
6. Rahman, M.I., Witrisal, K., Das, S.S., Fitzek, F.H.P., Olsen, O., Prasad, R.: Optimum pre-DFT combining with cyclic delay diversity for OFDM based WLAN systems. In: IEEE 59th Vehicular Technology Conference (VTC 2004-Spring), vol. 4, pp. 1844–1848 (May 2004)
7. Santamaría, I., Elvira, V., Vía, J., Ramírez, D., Pérez, J., Ibáñez, J., Eickhoff, R., Ellinger, F.: Optimal MIMO transmission schemes with adaptive antenna combining in the RF path. In: 6th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland (August 2008)
8. Vía, J., Elvira, V., Santamaría, I., Eickhoff, R.: Analog antenna combining for maximum capacity under OFDM transmissions. In: IEEE International Conference on Communications (ICC 2009), Dresden, Germany (June 2009)
9. Vía, J., Elvira, V., Santamaría, I., Eickhoff, R.: Minimum BER beanforming in the RF domain for OFDM transmissions and linear receivers. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2009), Taipei, Taiwan (April 2009)
10. Vía, J., Santamaría, I., Elvira, V., Eickhoff, R.: A General Criterion for Analog Tx-Rx Beamforming under OFDM Transmissions. IEEE Transactions on Signal Processing 58(4), 2155–2167 (2010)

Optimal Channel and Power Allocation for Secondary Users in Cooperative Cognitive Radio Networks

(Invited Paper)

Mario Bkassiny and Sudharman K. Jayaweera

Dept. of Electrical and Computer Engineering
University of New Mexico
Albuquerque, NM 87131-0001, USA
{bkassiny,jayaweera}@ece.unm.edu

Abstract. Cognitive radios are a natural evolution of Software Defined Radios (SDRs) that are supposed to be equipped with the ability to learn their RF environment and reconfigurability. A cognitive radio can communicate over a primary user's channel as long as the introduced interference does not degrade the primary Signal-to-Interference-plus-Noise-Ratio (SINR) below its minimum Quality of Service (QoS) requirement. In this paper, we employ cooperation in data transmission in order to increase the secondary transmit power limit. We present an optimal power allocation scheme for secondary users in order to achieve maximum SINR. We show that the optimal channel assignment problem that maximizes the sum-rate can be solved via the so-called Hungarian algorithm at a cubic complexity order. Also, we develop a suboptimal algorithm that permits to solve the channel assignment problem with a quadratic complexity order and with a slight performance degradation compared to that of the optimal solution.

1 Introduction

Most of RF spectrum below 6 GHz is historically owned by licensed users/services. Thus, the spectrum opportunities for the introduction of new wireless services are very limited [1]. With the increase in demand for higher capacities in existing communication systems, as well as for new wireless services, a solution is needed to overcome the problem of saturation of the spectrum. Cognitive radio is suggested as a promising solution after an observation of the spectrum usage, where it turns out that most licensed channels are not used by their owners most of the time, and some channels could handle a higher level of interference based on the Quality of Service (QoS) requirement of their users. According to [2], cognitive radio presents *intelligent* techniques to make efficient use of the spectrum by filling the spatial and temporal spectrum holes, without affecting the performance requirements of primary users. In this context, various research has been made to enhance the performance of cognitive radio systems, and it has been noted that significant

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 180–191, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

improvement can be achieved by applying the concept of *cooperation* to cognitive systems. Earlier, [3], [4] and [5] showed that cooperation can overcome the limitations of wireless systems by increasing the spatial diversity.

Previously, node cooperation has been applied for spectrum sensing in cognitive radio networks [6] where cognitive users cooperate to determine the spectral and/or temporal holes in the spectrum, so that cognitive devices will have a better estimate of the channel status, which reduces the excessive interference and collision risk with the primary licensed users [7], [8]. In these existing proposals, once cognitive users estimate the status of a channel, they communicate without cooperation.

In this paper, on the other hand, we present a cooperative design similar to the *cognitive relay* model in [9]: Cognitive users cooperate with primary (licensed) users by relaying the primary signal to its destination. Under certain channel conditions, this cooperation enables the secondary user to achieve a higher SINR without violating the primary user's QoS. In addition, such cooperative communication introduces diversity in the primary link helping the primary user to achieve its required QoS when its channel suffers from severe channel fading.

The motivation behind this model is due to the power constraints that a primary user imposes on a secondary cognitive user. We apply cooperation in order to increase the secondary transmit power. Thus, we develop a power allocation scheme that determines the amount of power spent by every secondary user to send both its private and relayed signals. The proposed power allocation scheme can be used in conjunction with any given channel assignment, and is optimal in the sense of maximizing the secondary transmission rate subject to a given primary QoS requirement. However, we note that the optimal power that maximizes the secondary SINR does not necessarily lead to maximum sum-rate achieved by the joint system made of primary and secondary users. Yet, our objective in this work is to maximize the spectrum utilization over all channels subject to the constraint of minimum primary QoS. Hence, we choose to allocate channels to the secondary users such that the sum-rate is maximized while power is chosen so that secondary SINR is maximized within each channel allocation.

We present two channel assignment methods that have polynomial complexity. The first, the optimal channel assignment method, forms a matching between primary and secondary users subject to maximizing the sum-rate, and is denoted as the Centralized Channel Assignment. The second method is a heuristic algorithm in which primary users are picked randomly and an optimal cooperative secondary user is assigned.

The remainder of this paper is organized as follows. In section 2, we develop the system model. In section 3, we derive the optimal power allocation scheme. Sections 4.1 and 4.2 present the optimal and suboptimal channel assignment methods, respectively. The simulation results are shown in section 5, and we conclude this paper in section 6.

2 System Model

The assumed dynamic spectrum sharing (DSS) cognitive radio system consists of K_p primary users (i.e. K_p licensed channels), K_s secondary transmitters, and 1 primary and 1 secondary receivers (base stations). The users are indexed using the set $\mathcal{K} = \mathcal{K}_p \cup \mathcal{K}_s$, where $\mathcal{K}_p = \{1, ..., K_p\}$ and $\mathcal{K}_s = \{K_p + 1, ..., K_p + K_s\}$ are the indices of the primary and secondary users, respectively. P_k denotes the transmit power of user k to send its *own* signal. In our proposed model, a cognitive secondary user will cooperate with a primary user by sending the primary user's signal in superposition with its own signal. $q_{j,i}$ denotes the transmit power of the cognitive user j ($j \in \mathcal{K}_s$) to send the signal of the primary user i ($i \in \mathcal{K}_p$), i.e. the total transmit power of the cognitive user j is equal to $P_j + q_{j,i}$, where we assume that at any given time each secondary user only cooperates with at most a single primary user. $h_{m,n}$ represents the channel fading coefficient between users m and n, h_{pk} is the channel fading coefficient between user k and the primary receiver, h_{sk} is the channel fading coefficient between user k and the secondary receiver. We denote the instantaneous SINR's of user $k \in \mathcal{K}$ at the primary and the secondary receivers as γ_{pk} and γ_{sk}, respectively. Also, we define $[x]^+ \triangleq \max\{0, x\}$.

In this system, each secondary cognitive user wants to communicate with the secondary receiver on any one of the available K_p primary channels. To achieve this communication, the secondary user will cooperate with the primary user to whom the selected channel belongs.

At any given time, a secondary user is assumed to be only capable of communicating over one chosen channel. The scheduling function $\phi : j \to i$ ($j \in \mathcal{K}_s$ and $i \in \mathcal{K}_p \bigcup \{0\}$) forms a mapping between the cognitive user j and its corresponding cooperative primary channel i. When $\phi(j) = 0$ this will indicate that user j is not cooperating with any primary user. Alternatively, the scheduling function ϕ can be defined using the assignment vector $\varPhi = [\phi(K_p + 1), ..., \phi(K_p + K_s)]^T$ which has $[K_s - K_p]^+$ zero elements (representing the secondary users that cannot be assigned to any primary channel when the number of primary channels is limited), and $\phi(u) \neq \phi(v)$ for any $(u, v) \in \mathcal{K}_s \times \mathcal{K}_s$ with $u \neq v$ and $\phi(u)\phi(v) \neq 0$.

Let $b_k^{(l)}$ be the l-th symbol from transmitter $k \in \mathcal{K}$. The transmission of every primary symbol is done in two stages: In the first step, primary i transmits its m-th symbol $b_i^{(m)}$ with a power αP_i (where $\alpha \in [0, 1]$) to secondary user j which generates the estimate $\hat{b}_i^{(m)}$. Secondary users are assumed to be full-duplex devices, so the secondary user is capable of transmitting its m'-th private symbol $b_j^{(m')}$ during the first step at a power that does not degrade the primary QoS. During the second step, primary user i again transmits the same symbol $b_i^{(m)}$ at a power $(1 - \alpha) P_i$ and the secondary cognitive user transmits both $\hat{b}_i^{(m)}$ and its private symbol $b_j^{(m'+1)}$ with respective powers $q_{j,i}$ and P_j. The transmission of the primary symbol in two time stages decreases the transmission rate, but as shown in [4], this decrease in transmission rate can be compensated by the reduction in symbol-error probability under certain channel conditions.

In the following sections, we will make the so-called *genie assumption* [2] which implies that the primary message is known to the cognitive user [10]. Thus, in computing the received SINR and the system throughput, we will assume that the transmission is done in one time slot.

3 Power Allocation Scheme

In cognitive systems, a power constraint is imposed on the secondary user so that the SINR of the incumbent primary user i doesn't drop below its minimal SINR requirement denoted by $\overline{\gamma}_{pi}$ that is determined by the QoS requirement of the primary user on channel i. The SINR at the primary receiver when secondary user j selects channel i (i.e. when $\phi(j) = i$) is:

$$\gamma_{pi} = \frac{P_i h_{pi}^2 + q_{j,i} h_{pj}^2}{P_j h_{pj}^2 + N_0} \ , \tag{1}$$

where N_0 is the average noise power at the receiver. Since this SINR should be greater than the threshold $\overline{\gamma}_{pi}$, by solving for P_j so that $\gamma_{pi} \geq \overline{\gamma}_{pi}$, we obtain the maximum allowable transmit power of the cognitive user j to send its own signal:

$$P_j \leq \min\left\{ \overline{P}_j - q_{j,i}, \left[\frac{P_i h_{pi}^2 - \overline{\gamma}_{pi} N_0 + q_{j,i} h_{pj}^2}{\overline{\gamma}_{pi} h_{pj}^2} \right]^+ \right\} \triangleq \xi_{j,i} \ , \tag{2}$$

where $\overline{P}_j$ is the maximum total transmit power of secondary user j such that $P_j + q_{j,i} \leq \overline{P}_j$. When $\phi(j) = i$, the SINR at the secondary receiver in channel i is:

$$\gamma_{sj} = \frac{P_j h_{sj}^2}{P_i h_{si}^2 + q_{j,i} h_{sj}^2 + N_0} \ . \tag{3}$$

The objective of the power allocation problem is to find the optimal values P_j^* and $q_{j,i}^*$ such that:

$$\left(q_{j,i}^*, P_j^*\right) = \arg \max_{(q_{j,i}, P_j)} \gamma_{sj} \tag{4}$$

subject to:

$$\begin{array}{rl} P_j \leq & \overline{P}_j - q_{j,i} \\ P_j \leq & \frac{q_{j,i}}{\overline{\gamma}_{pi}} + \tau \\ P_j > & 0 \\ q_{j,i} \geq & 0 \end{array} \ , \tag{5}$$

where $\tau = \frac{P_i h_{pi}^2 - \overline{\gamma}_{pi} N_0}{\overline{\gamma}_{pi} h_{pj}^2}$, $i \in \mathcal{K}_p$ and $j \in \mathcal{K}_s$. The shaded area in Fig. 1 represents the feasibility region defined by (5). For any given channel assignment, we

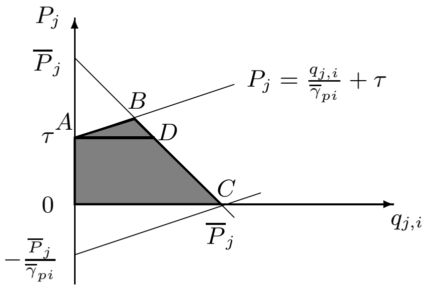

P_j
$\overline{P}_j$
B
$P_j = \frac{q_{j,i}}{\overline{\gamma}_{pi}} + \tau$
A
τ
D
C
0
$\overline{P}_j$
$q_{j,i}$
$-\frac{\overline{P}_j}{\overline{\gamma}_{pi}}$

Fig. 1. Feasibility Region for maximizing γ_{sj}

characterize the optimal power allocation solution in (6), and the derivation is shown in Appendix A.

$$\left(q^*_{j,i}, P^*_j\right) = \begin{cases} \left(0, \min\{\overline{P}_j, \tau\}\right) & \text{if} \quad \tau \geq \min\{\overline{P}_j, \tau_1\} \\ \left(\lambda_i, \overline{P}_j - \lambda_i\right) & \text{if} \; -\frac{\overline{P}_j}{\overline{\gamma}_{pi}} < \tau < \min\{\overline{P}_j, \tau_1\} \\ (0,0) & \text{if} \quad \tau \leq -\frac{\overline{P}_j}{\overline{\gamma}_{pi}} \end{cases} , \tag{6}$$

where $\tau_1 = \frac{P_i h_{si}^2 + N_0}{\overline{\gamma}_{pi} h_{sj}^2}$ and $\lambda_i = \frac{\overline{\gamma}_{pi}}{1+\overline{\gamma}_{pi}} \left(\overline{P}_j - \tau\right)$.

Note that for large $\overline{\gamma}_{pi}$, it is more likely to have $\tau < -\frac{\overline{P}_j}{\overline{\gamma}_{pi}}$ so that the secondary does not get to transmit any signal.

On the other hand, the optimal power allocation for non-cooperative cognitive systems is simply $\left(q^*_{j,i}, P^*_j\right) = \left(0, \min\left\{\overline{P}_j, [\tau]^+\right\}\right)$.

4 Channel Assignment Algorithms

4.1 Centralized Channel Assignment

The cognitive cooperative communications scheme that we introduced in section 2 allows each primary user to cooperate with a secondary user that is sharing its licensed spectrum. The cognitive receiver, which is assumed to know the channel state information (CSI), is assumed to be responsible for assigning a primary channel to each cognitive secondary user.

Since the optimal solution in (6) depends on combination $(i,j) \in \mathcal{K}_p \times \mathcal{K}_s$, some cooperative combinations may lead to a higher secondary SINR than other combinations. Since we are interested in maximizing the transmission rate of the combined spectrum-sharing system, and in driving the primary SINR to its minimum requirement when it drops below its QoS (due to fading for example), we define the objective function $R_s(\Phi) = \sum_{i \in \mathcal{K}_p} R_i$ to be the sum of primary and secondary rates for all users, where R_i is the sum-rate on channel i defined as:

$$R_i \triangleq R_{p,i} + R_{s,i} \triangleq \log_2\left(1 + \gamma_{pi}\right) + \log_2\left(1 + \gamma_{sj}\right) ,$$

where $j = \phi^{-1}(i)$ and $R_{p,i}$ and $R_{s,i}$ are the primary and secondary rates on channel i, respectively.

Thus, the problem of optimal channel assignment is solved by finding the assignment vector Φ^* such that $\Phi^* = \arg\max_{\Phi} \sum_{i \in \mathcal{K}_p} R_i$. Because each primary user can share its spectrum with at most one secondary user at a time, and each secondary user can transmit over one channel at a time, the channel assignment problem becomes similar to the assignment problem in a weighted bipartite graph[1] where primary and secondary users constitute the two disjoint sets of vertices, and the edge weight between primary i and secondary j is equal to R_i. Figure 2 shows an example of a system consisting of $K_p = 4$ primary and $K_s = 4$ secondary users, with the corresponding edge weights R_i. In solving the channel assignment problem, our goal is to find the optimal matching between the elements of the two sets so that we maximize the sum of the weights of the matching edges (so that we maximize the sum-rate $R_s(\Phi)$)[2].

According to [11], this assignment problem is a special case of the Hitchcock problem, and it can be solved by the *Hungarian algorithm* which is proposed by Khun [12]. The *Hungarian algorithm* solves the weighted matching problem for a complete bipartite graph. A complete bipartite graph has the same number of elements in both sets, but according to [11], we can always assume that a bipartite graph is complete by setting the weights of the missing edges to be equal to 0, and [13] shows that we still get the optimal solution for the bipartite graph by applying this modification.

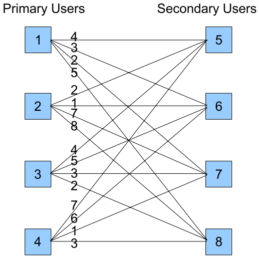


Fig. 2. Bipartite Graph Representation

Algorithm 1 gives the optimal channel assignment using the Hungarian algorithm as described in [13]. In the following, we apply this algorithm to the example in Fig. 2 where $\mathcal{K}_p = \{1, 2, 3, 4\}$ and $\mathcal{K}_s = \{5, 6, 7, 8\}$. We define the weight matrix $\mathbf{W}$ in (7).

---

[1] A bipartite graph is a graph whose vertices belong to two disjoint sets, such that every vertex is connected to at most one vertex from the other set.

[2] This optimization method can be used to find the optimal channel assignment for cognitive non-cooperative systems by using the non-cooperative optimal power allocation solution given at the end of section 3. In general, it can compute the optimal channel assignment for any cognitive cooperative system after having determined the appropriate power allocation scheme.

In step 1, we initialize $(u_1, u_2, u_3, u_4) = (5, 8, 5, 7)$ and $(v_1, v_2, v_3, v_4) = (0, 0, 0, 0)$. In step 2 we compute $C^{(1)}$ shown in (7). The maximum matching M of G has 3 edges (marked by the stars in $C^{(1)}$) and this matching is not optimal. Thus, in step 4 we form the vertex cover $Q = \{3, 5, 8\}$, to obtain $\epsilon = 1$, and we update $(u_1, u_2, u_3, u_4) = (4, 7, 5, 6)$ and $(v_1, v_2, v_3, v_4) = (1, 0, 0, 1)$. The corresponding $C^{(2)}$ is shown in (7). The maximum matching of G (which maps nodes 1, 2, 3 and 4 to 8, 7, 6 and 5, respectively) has 4 edges and it is the optimal matching for this graph.

$$\mathbf{W} = \begin{bmatrix} 4 & 3 & 2 & 5 \\ 2 & 1 & 7 & 8 \\ 4 & 5 & 3 & 2 \\ 7 & 6 & 1 & 3 \end{bmatrix}, \mathbf{C}^{(1)} = \begin{bmatrix} 1 & 2 & 3 & 0 \\ 6 & 7 & 1 & 0^* \\ 1 & 0^* & 2 & 3 \\ 0^* & 1 & 6 & 4 \end{bmatrix} \text{ and } \mathbf{C}^{(2)} = \begin{bmatrix} 1 & 1 & 2 & 0^* \\ 6 & 6 & 0^* & 0 \\ 2 & 0^* & 2 & 4 \\ 0^* & 0 & 5 & 4 \end{bmatrix} \quad (7)$$

We use the code described in [14] to find the maximum weight matching. This code can compute the optimal matching for a 100-by-100 matrix in 120ms when operating on a 2.4GHz processor.

Algorithm 1. Centralized Optimal Channel Assignment

```
Given $\mathcal{K}_p$ and $\mathcal{K}_s$ (with cardinality $k$ for each set). Let $\mathbf{W} = [w_{ij}] \in \mathbb{R}^{k \times k}$ be the weight matrix where $w_{i,j} = R_i$ with $\phi(j) = i$.
1. Initialize two labels $u_i = \max_{j \in \{1,...,k\}} w_{ij}$ and $v_j = 0$ for $i, j = 1, ..., k$.
2. Obtain the excess matrix $\mathbf{C} = [c_{ij}] \in \mathbb{R}^{k \times k}$ such that $c_{ij} = u_i + v_j - w_{ij}$
3. Find the subgraph $G$ consisting of vertices $i$ and $j$ satisfying $c_{ij} = 0$ and the corresponding edge $e_{ij}$. Find the maximum matching $M$ in $G$.
If M is perfect matching with $k$ edges, go to step 5.
4. Let $Q$ be a vertex cover of $G$, and let $R = \mathcal{K}_p \bigcap Q$ and $T = \mathcal{K}_s \bigcap Q$.
A vertex cover contains at least one endpoint of each edge of a graph.
Find $\epsilon$ satisfying $\epsilon = \min\{c_{ij} : x_i \in \mathcal{K}_p - R, y_j \in \mathcal{K}_s - T\}$.
Decrease $u_i$ by $\epsilon$ for the rows of $R^c$ and increase $v_j$ by $\epsilon$ for the columns of $T$. Then go to step 2.
5. $M$ is the optimal assignment solution when $M$ is perfectly matched with $k$ edges
```

4.2 Heuristic Assignment Method

The Hungarian algorithm presented above solves the optimal matching problem for a complete weighted bipartite graph with $2n$ vertices in $\mathcal{O}(n^3)$ arithmetic operations [11]. Since we can assume that any bipartite graph is complete if we set the weights of the missing edges to be equal to 0, then the complexity order of the optimal channel assignment in our system is $\mathcal{O}\left[(\max\{K_p, K_s\})^3\right]$.

To reduce the computational complexity, in the following we propose a heuristic algorithm (Algorithm 2) similar to [15] with a lower complexity order to solve the channel assignment in large systems. We consider K_p primary and K_s secondary users, and find the channel assignment between these nodes. Algorithm 2 is applied when $K_p \leq K_s$, and an analogous algorithm can be deduced for the case when $K_p > K_s$, as we will show later. As will be shown, this algorithm will have at most quadratic complexity in $\max\{K_p, K_s\}$.

The Algorithm 2 randomly selects a primary user $i \in \mathcal{K}_p$ and its corresponding optimal cooperating cognitive device $j^*(i) \in \mathcal{K}_s$ is found. Then, i and $j^*(i)$ are removed from the sets $\mathcal{K}_p$ and $\mathcal{K}_s$, respectively, and the same procedure is repeated with the remaining elements. In practice, when $K_p \leq K_s$, all available secondary users simultaneously scan a randomly selected primary channel and obtain the CSI and the value of P_i. We assume that the CSI stays fixed for the duration of a block. Once the cognitive secondary system knows the transmit primary power P_i, every secondary user computes the γ_{pi} and γ_{sj} using (1) and (3), respectively. These SINR values can be known after solving for the optimal $q_{j,i}$ and P_j using (6). Next, the set $\{R_i\}_{j\in\mathcal{K}_s}$ is computed and the cognitive user $j^*(i) = \arg\max_{j\in\mathcal{K}_s} R_i$ is selected to cooperate with primary user i.

Similarly, if $K_p > K_s$, a cognitive user is selected randomly from the set $\mathcal{K}_s$, and this user scans all available primary channels and chooses to cooperate with the channel $i^*(j) = \arg\max_{i\in\mathcal{K}_p} R_i$. Then, $i^*(j)$ and j are removed from the sets $\mathcal{K}_p$ and $\mathcal{K}_s$, and the same procedure is repeated until all secondary users are exhausted.

Algorithm 2. Heuristic Assignment Method ($K_p \leq K_s$)

```
1. Randomly pick a primary user $i \in \mathcal{K}_p$.
2. Calculate $j^*(i) = \arg\max_{j\in\mathcal{K}_s}\{\log_2(1+\gamma_{pi}) + \log_2(1+\gamma_{sj})\}$ when $j$ cooperates with $i$ ($\phi(j) = i$).
3. Remove $i$ and $j^*$ from the set $\mathcal{K} = \mathcal{K}_p \bigcup \mathcal{K}_s$ and repeat the same procedure with the remaining elements until $\mathcal{K}_p = \emptyset$.
```

Algorithm 2 ensures that all R_i values are considered in the computation. However, it reduces the assignment complexity to the order of $\mathcal{O}(K_p K_s)$, since the number of comparisons is equal to $\sum_{i=0}^{K_p-1}(K_s - i)$ when $K_p \leq K_s$.

5 Numerical Results

We simulate a system consisting of $K_p = 3$ primary users and $K_s = 5$ secondary users. Throughout all simulations, we assume all fading coefficients to be i.i.d. Rayleigh distributed with normalized power $\mathbb{E}[h^2] = 1$. We let $P_i = 1W$, for $i \in \mathcal{K}_p$, and assume $\overline{P}_j$ to be the same for all $j \in \mathcal{K}_s$. The average noise power at the receivers is $N_0 = 0.1W$, and all primary users have the same SINR requirement $\overline{\gamma}_{pi} = \overline{\gamma}_p$. We assume that secondary users have knowledge of the primary message.

In Fig. 3 we plot the average sum-rate $\overline{R}_s$ versus $\overline{\gamma}_p$ subject to fixed $\overline{P}_j$. At any given $\overline{\gamma}_p$, we observe that the value of $\overline{R}_s$ that is achieved by cooperative cognitive systems is higher than $\overline{R}_s$ in non-cooperative cognitive systems. Also,

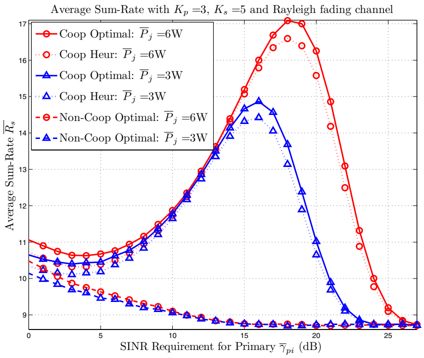


Fig. 3. Average Sum-Rate under Rayleigh fading subject to $\overline{P}_j$

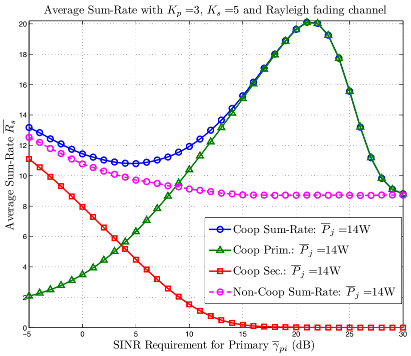


Fig. 4. Average Primary Rate under Rayleigh fading subject to $\overline{P}_j = 14\text{W}$

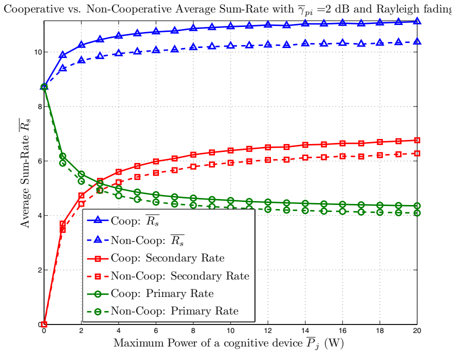


Fig. 5. Elementary Average Sum-Rate under Rayleigh fading

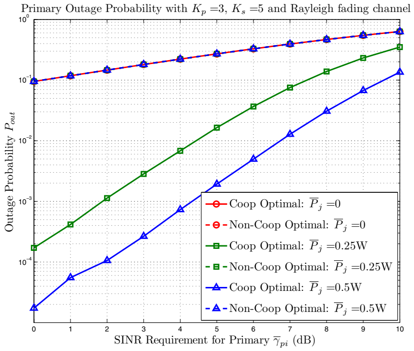


Fig. 6. Outage Probability of Primary Users

the performance of cooperative systems with heuristic assignment method is reasonably close to that of cooperative systems with optimal assignment method. Figure 4 shows that for large values of $\overline{\gamma}_p$, cognitive secondary users do not get to transmit because $\tau \leq -\frac{\overline{P}_j}{\overline{\gamma}_{pi}}$. Also, for $\overline{P}_j = 14W$, the average cooperative sum-rate is decreasing over the interval $[-5\text{ dB}, 5\text{ dB}]$ because it is dominated by the decreasing average secondary rate. As the secondary rate approaches 0, the average sum-rate becomes close to $K_p \log_2\left(1 + \overline{\gamma}_{pi}\right)$ for all $\overline{P}_j$ values that enable the primary to meet its SINR requirement.

Next, in Fig. 5, we plot the averages of R_s, $\sum_{1\in\mathcal{K}_p} R_{p,i}$ and $\sum_{1\in\mathcal{K}_p} R_{s,i}$ over fading for $\overline{\gamma}_{pi} = 2dB$. For any $\overline{P}_j$, we observe that cooperation increases the average sum-rate for primary and secondary users. In fact, the objective of this optimization is to increase γ_{sj} subject to maintaining $\gamma_{pi} \geq \overline{\gamma}_{pi}$. As we increase

$\overline{P}_j$, the average primary sum-rate decreases to $K_p \log_2 \left(1 + \overline{\gamma}_{pi}\right) = 4.11$, but it does not drop below its QoS requirement. We note also that the average sum-rate of the secondary user is not necessarily equal to 0 when the average sum-rate of the primary is less than its QoS requirement, because whenever the *instantaneous* primary SINR γ_{pi} is greater than $\overline{\gamma}_{pi}$, the secondary user gets to transmit at a non-zero rate, regardless of the *average* primary SINR which could be less than $\overline{\gamma}_{pi}$. Thus the average sum-rate of secondary users in a non-cooperative system is not identically zero when the average sum-rate of primary users is below the QoS requirement.

Next, we plot in Fig. 6 the primary outage probability defined as $P_{out} \triangleq \Pr\left\{\gamma_{pi} < \overline{\gamma}_{pi}\right\}$. This plot shows that cooperation reduces significantly the outage probability of primary users. In the absence of cooperation, the introduction of a cognitive user does not affect the primary outage probability because secondary users are not allowed to degrade the primary QoS requirements at any time. Hence the outage probability curves in Fig. 6 when $\overline{P}_j = 0$ coincide with the outage probability curves in non-cooperative cognitive scenarios with $\overline{P}_j > 0$. However, as can be observed through cooperation, cognitive users help to reduce the primary outage probability, as well as increasing their own transmission rate (as in Fig. 5).

6 Conclusion

In this paper, we have proposed a model that takes advantage of cooperative communications to improve spectrum utilization and primary outage performance of cognitive radio systems. Although cooperation has been widely used in cognitive radio for the purpose of spectrum sensing, our model applies cooperation in data transmission. We showed that our proposed technique could increase the transmission sum-rate of both primary and secondary users by means of increasing the primary channel diversity, and increasing the secondary transmission power limit. We derived an optimal and a heuristic channel assignment algorithm, as well as an optimal power allocation scheme for the proposed system. The channel assignment and power allocation algorithms can be applied independently to cognitive cooperative systems. In this paper, we applied the Centralized Channel Assignment to maximize the average sum-rate of the network, while the power allocation scheme guarantees maximum secondary SINR in every channel.

References

1. Zhang, Y., Leung, C.: Resource Allocation in an OFDM-based Cognitive Radio System. IEEE Transactions on Communications 57(7), 1928–1931 (2009)
2. Devroye, N., Vu, M., Tarokh, V.: Cognitive Radio Networks. IEEE Signal Processing Magazine, 12–22 (November 2008)
3. Zhang, W., Letaief, K.B.: Cooperative Communications for Cognitive Radio Networks. Proceedings of the IEEE 97(5), 878–893 (2009)

4. Sendonaris, A., Erkip, E., Aazhang, B.: User Cooperation Diversity: Part I. System Description. IEEE Transactions on Communications 51(11), 1927–1938 (2003)
5. Sendonaris, A., Erkip, E., Aazhang, B.: User Cooperation Diversity: Part II. Implementation Aspects and Performance Analysis. IEEE Transactions on Communications 51(11), 1939–1948 (2003)
6. Zheng, Y., Xie, X., Yang, L.: Cooperative Spectrum Sensing based on Blind Source Separation for Cognitive Radio. In: 1st International Conference on Future Information Networks 2009, Beijing, China, pp. 398–402 (October 2009)
7. Liu, Y., Yuan, D., Jiang, M., Yu, H., Xu, C., Zhao, P.: Cooperative Spectrum Sensing in Cognitive Networks. In: IEEE Region 10 Conference TENCON 2008, Hyderabad, India, pp. 1–6 (November 2008)
8. Matsui, M., Shiba, H., Akabane, K., Uehara, K.: A Cooperative Sensing Technique with Weighting based on distance between radio stations. In: 14th Asia-Pacific Conference on Communications 2008, Tokyo, Japan, pp. 1–4 (October 2008)
9. Simeone, O., Gambini, J., Bar-Ness, Y., Spagnolini, U.: Cooperation and Cognitive Radio. In: IEEE International Conference on Communications 2007, Glasgow, United Kingdom, pp. 6511–6515 (June 2007)
10. Devroye, N., Mitran, P., Tarokh, V.: Achievable Rates in Cognitive Radio Channels. IEEE Transactions on Information Theory 52(5), 1813–1827 (2006)
11. Papadimitriou, C.H., Steiglitz, K.: Combinatorial Optimization: Algorithms and Complexity, pp. 247–248. Dover Publications, Mineola (1998)
12. Kuhn, H.: The Hungarian Method for the Assignment Problem. Naval Research Logistics Quarterly 2, 83–97 (1955)
13. Choi, Y.-J., Kim, J., Bahk, S.: Downlink Scheduling with Fairness and Optimal Antenna Assignment for MIMO Cellular Systems. In: IEEE Global Telecommunications Conference 2004, Dallas, TX, pp. 3165–3169 (November -December 2004)
14. Hungarian Algorithm, `http://www.mathworks.com/matlabcentral/leexchange/11609-hungarian-algorithm`
15. Chang, Y.-J., Tao, Z., Zhang, J., Kuo, C.-C.: A Graph-Based Approach to Multi-Cell OFDMA Downlink Resource Allocation. In: IEEE Global Telecommunications Conference 2008, New Orleans, LO, pp. 1–6 (December 2008)

A Derivation of the Optimal Power Allocation

The feasibility region in Fig. 1 shows that the optimal solution depends on the range of τ. In order to solve this optimization problem, we first note that γ_{sj} in (3) increases by increasing P_j and by decreasing $q_{j,i}$.

Case 1: If $\tau \geq \overline{P}_j$, the optimal solution is $\left(q^*_{j,i}, P^*_j\right) = \left(0, \overline{P}_j\right)$.

Case 2: If $0 \leq \tau < \overline{P}_j$, and referring to Fig. 1, we see that for any $q_{j,i} \in [0, \overline{P}_j]$, γ_{sj} is maximized when the solution belongs to the segments $[AB]$ or $[BC]$. That's because P_j is maximized (for every $q_{j,i}$) by selecting a feasible point from these segments.

Let $\lambda_i \triangleq \frac{\overline{\gamma}_{pi}}{1+\overline{\gamma}_{pi}}\left(\overline{P}_j - \tau\right)$ be the abscissa of point B. For any $P_j \in \left[\tau, \overline{P}_j - \lambda_i\right]$, we see that all feasible points from the segment $[BD]$ are suboptimal when compared to the points of segment $[AB]$ which has the same values of P_j but with a smaller $q_{j,i}$. Note that we have rejected the region where $P_j < \tau$ because it yields suboptimal γ_{sj} when compared to the point $(0, \tau)$.

Therefore, the optimal solution in this case is on the segment $[AB]$. The secondary SINR expression over this segment is $\gamma_{sj} = \frac{\left(\frac{q_{j,i}}{\overline{\gamma}_{pi}} + \tau\right) h_{sj}^2}{P_i h_{si}^2 + q_{j,i} h_{sj}^2 + N_0}$. Computing its partial derivative with respect to $q_{j,i}$, we get:

$$\frac{\partial \gamma_{sj}}{\partial q_{j,i}} = \frac{P_i h_{sj}^2 h_{si}^2 + N_0 h_{sj}^2 - \tau h_{sj}^4 \overline{\gamma}_{pi}}{\overline{\gamma}_{pi} \left(P_i h_{si}^2 + q_{j,i} h_{sj}^2 + N_0\right)^2} \ . \tag{8}$$

Let $\tau_1 \triangleq \frac{P_i h_{si}^2 + N_0}{\overline{\gamma}_{pi} h_{sj}^2}$. If $\tau < \tau_1$, then $\frac{\partial \gamma_{sj}}{\partial q_{j,i}} > 0$ and the optimal solution is $\left(q_{j,i}^*, P_j^*\right) = \left(\lambda_i, \overline{P}_j - \lambda_i\right)$. Otherwise, the optimal solution will be $\left(q_{j,i}^*, P_j^*\right) = (0, \tau)$.

Case 3: If $-\frac{\overline{P}_j}{\overline{\gamma}_{pi}} < \tau < 0$, and using the same analysis of Case 2, the optimal solution belongs to the line segment formed by the points $\left(-\tau \overline{\gamma}_{pi}, 0\right)$ and $\left(\lambda_i, \overline{P}_j - \lambda_i\right)$. But $\tau < 0 \leq \tau_1$, then γ_{sj} is a monotonically increasing function of $q_{j,i}$ and the optimal solution is $\left(q_{j,i}^*, P_j^*\right) = \left(\lambda_i, \overline{P}_j - \lambda_i\right)$.

Case 4: If $\tau \leq -\frac{\overline{P}_j}{\overline{\gamma}_{pi}}$, we see in Fig. 1 that the problem does not have a feasible solution. This corresponds to the case when the primary QoS could not be met even with the help of the secondary cooperation. In this case, we set $\left(q_{j,i}^*, {P_j}^*\right) = (0, 0)$ so that the secondary user does not relay any amount of power for the primary user unless it is allowed to transmit its own signal for some $P_j > 0$.

“User Authentication Method and Implementation Using a Three-Axis Accelerometer”

Alexandros Zaharis, Adamantini Martini, Panayotis Kikiras, and George Stamoulis

Department of Computer & Communication Engineering,
University of Thessaly
Greece, Volos
{alzahari,admartin,kikirasp,georges}@inf.uth.gr
http://wssl.inf.uth.gr

Abstract. The rapid growth of accelerometer use on consumer electronics has brought an opportunity for unique user authentication. We present an efficient recognition algorithm for such interaction using a single three-axis accelerometer. Unlike common user authentication methods which require memorizing complex phrases and are prone to physical attacks, our method requires a single training sample for a gesture pattern which allows users to authenticate themselves in a fast and secure manner. Our work imitates the use of physical handwritten signatures, which are a common authentication technique and tries to integrate them in a digital form. The presented method aims at providing easy to remember personalized gesture passwords through the muscle memory ability of the human body. An implementation using the wii remote sensor, along with identification results for different users is presented as a proof of concept.

Keywords: gesture recognition, three axis accelerometer sensor, user authentication.

1 Introduction

An increasing number of home electronic devices and mobile phones are equipped with accelerometers, enabling a device to “sense” how it is physically manipulated by the user. In our work, we use the word “gesture” to refer to the physical interaction of the user with the device and the word “signature” to refer to a three dimensional movement which produces easily identifiable results that can authenticate a user.

In the literature there are a lot of studies regarding the use of accelerometers as a tool for recognizing gestures [5-8]. Within this paper we will try to demonstrate that the recognition of a single, easy to remember three dimensional signature-like gestures for user authentication is feasible.

For example, a user can “shake” a phone in a special way to log in or a wii remote to load personalized data for a game. While many paradigms exist for user authentication, including password [9], biometrics [10-12], speech [13], and handwriting [14], accelerometer - based signature recognition has its unique value for user authentication because of its low cost, high efficiency, and no form factor change. These properties make it highly suitable for implementation on resource constrained devices, such as mobile phones and TV remotes or handheld game consoles.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 192–202, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

The goal of our work is to investigate the feasibility and usability of a three dimensional signature recognition based on a single tri-axis accelerometer[5], because either it is privacy-insensitive data, like personalized configurations on a game, or privacy-sensitive data like personal contacts stored in a mobile phone, the resilience to attacks and usability are dominating concerns.

In order to succeed in the aforementioned goal, a unique method and implementation is presented in *Section 4*. In *Section 5*, a series of tests and experiments is presented in order to prove the usability, security and effectiveness of the proposed method. Finally, the paper concludes with some useful remarks and our envisioned future research.

2 Related Work

Most user authentication methods are based on either what properties the user has, e.g. fingerprint [10], face [11] and iris [12], or what the user knows, e.g. password [9], or both, e.g. speaker verification [13] and handwritten signature recognition [14]. The work in [15-17] considers gesture as behavioural biometrics where the user has and attempts to verify or recognize the user identity based on a fixed gesture performed, e.g. a simple arm swing in [15]. Others allow the user to create any physical manipulation of the device as the authenticating gesture [5], with an error rate close to 3% and a single training sample. Notably, the basic method in [17] has over 14% equal error rate when not as many training samples are used. Moreover, the authors did not investigate how robust their methods are against attackers imitating the user, which is an important issue for every authentication method.

The goal of [16] is targeted on recognizing a user out of a small number of users sharing a device. The work achieved an accuracy of about 95% with a large number of training samples while the user had to perform a given gesture in a highly constrained manner, e.g. exact timing with real-time visual feedback. Related to our use of accelerometers, the work in [18] employed accelerometers to recognize the user with the gait pattern as behavioural biometrics.

What is unique about our proposed authentication method and implementation is the fact that a single 3D accelerometer device is used in order to authenticate the user with only three training samples. The notion of muscle memory, along with the physical signature, (a familiar motion to the user) lead to high identification rates while at the same time provide the user with an easy to remember, unique identifier. The identification algorithm digitalizes physical signature forensic techniques in order to distinguish unique marks and patterns on the performed signature in order to safely identify a user.

3 Muscle Memory and Handwritten Signature

This paragraph presents the two main principles/practices that facilitating the use of data produced by a 3D- axis accelerometer in a user authentication method.

3.1 Muscle Memory

When an active person repeatedly trains movement, often of the same activity, in an effort to stimulate the mind’s adaptation process, the outcome is to induce physiological changes which attain increased levels of accuracy through repetition. Even though the process is really brain-muscle memory or motor memory, the colloquial expression "muscle memory" is commonly used. Individuals rely upon the mind's ability to assimilate a given activity and adapt to the training. As the brain and muscle adapts to training, the subsequent changes are a form or representation of its muscle memory. There are two types of motor skills involved in muscle memory: fine and gross. Fine motor skills are very minute and small skills similar to those that we perform with our hands such as brushing teeth, combing hair, using a pencil or pen to write or sign, touch typing, playing some musical instruments, or even playing video games. Gross motor skills are those actions that require large body parts and large body movements as in sports such as bowling, baseball, rowing, basketball, golf, martial arts, and tennis, and activities such as driving a car (especially one with a manual transmission), piloting aircraft, playing some musical instruments, and marksmanship. Muscle memory is fashioned over time through repetition of a given suite of motor skills and the ability through brain activity to inculcate and instil it until they become automatic. To the beginner, activities such as signing are not as easy as they look. As one reinforces those movements through repetition, the neural system learns those fine and gross motor skills to the degree that one no longer needs to think about them, but merely to react and perform appropriately. In this sense, the muscle memory process is an example of automating an O.O.D.A [1] loop insofar as one learns to Observe, Orient, Decide, and Act.

When one picks up a pen to sign, automatically has a certain motion, style, number of strokes without requiring conscious thought about each movement. Other forms of rather elaborate actions that have become automatic include speech. It is said that it takes about 740 [1-2] of the same motions for your muscles to "memorize" the movements almost perfectly. Our method uses the already trained muscle memory of an individual performing a physical signature in order to achieve user authentication. The user has to use the 3- axis accelerometer as a pen in order to form his unique signature. As it will be demonstrated, due to user's previous training to the same movement in the real world the results are very accurate and can be used for user authentication.

3.2 Handwriting Forensics

The examination of handwriting to assess potential authorship proceeds from the principle of identification which can be expressed as: "Two writings are the product of one person if the handwriting characteristics, when taken in combination, are sufficiently individual and there are no fundamental unexplainable differences."

Generally, there are three stages in the process of examination [4]. In brief, they are:

1. Analysis: The questioned and the known items are analyzed and broken down to directly perceptible characteristics.
2. Comparison: The characteristics of the questioned item are then compared against the known standard.
3. Evaluation: Similarities and/or differences in the compared properties are evaluated and this determines which ones are valuable for a conclusion. This depends on the uniqueness and frequency of occurrence in the items.
4. Optionally, the procedure may involve a fourth step consisting of verification/validation or peer review.

Our method combines the knowledge of anthropology and document forensics science in order to produce an accurate user authentication method with a single 3D axis accelerometer.

4 Proposed Signature Recognition Method Based On a 3-Axis Accelerometer

The proposed Signature Recognition Method consists of two phases. In the first phase the user trains / registers his signature. The second phase consists of the user authentication module, where the user forms the signature and asks for validation after providing his username.

4.1 Phase 1: Training / User Registration

The first step in every user authentication process is registering the user. This phase is crucial for the success of a user authentication technique, as it must be robust, easy to understand by every user, fast (complete in a few steps) and accurate. The proposed method satisfies all the abovementioned aspects of a successful authentication method with an intuitive utilization of a single low-cost sensor.

Figure 1 illustrates the user registration process which correlates unique username chosen by the user with a gesture password (3D Signature). During this process a textual password is also generated along with a unique hash value that can act as a digital signature:

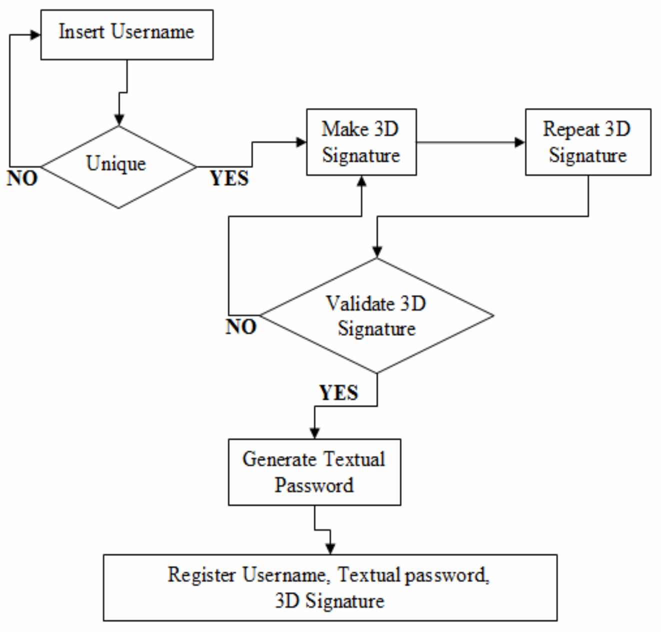


Fig. 1. User registration process

Step 1 – The user registration process begins by choosing a unique username.

***Step 2* –** After the username is chosen the user is asked to perform a 3D signature movement in a form of waving gesture in the three dimensional space. The capturing of the motion begins and ends with the sensor staying still for a few seconds. Three sets of acceleration values are collected, representing the x, y, z axis acceleration during the gesture. The gesture is then further analyzed in order to provide data that can be stored and compared to authenticate a user.

The data used for authentication are:

1. Elapsed time for the completion of the gesture.
2. The gesture is divided in smaller equal duration parts (time slots) for which the maximum and minimum acceleration values per axis is collected.
3. Starting sensor position (pitch, roll values)
4. Ending sensor position (pitch, roll values)
5. Total maximum and minimum acceleration value per axis is collected.

***Step 3* –** The user is asked to repeat the 3D signature in order to be validated. The above mentioned characteristics are compared to the newly acquired. If there is a match (with some tolerance) then the signature is validated.

***Step 4* –** After the validation has taken place a textual password along with a digital signature is being generated. The textual password is an 8 digit phrase (not random) created by numbers and characters which are directly seeded by the results acquired due to the 3D signature movement.

***Step 5* –** The username, textual password generated and 3D signature characteristics are stored and the user is registered.

4.2 Phase 2: User Authentication

In order to authenticate a user, his/her username and password must be provided. The password might be something the user “knows” (ex. text passwords) or something the user “has” (ex. biometry). Our users must provide a username and then form his/her personal 3D signature in order to be authenticated. The user is given three attempts to achieve authentication or his/her account else her account will be temporarily blocked. Optionally the user can login with the textual password generated after three failed 3D password attempts.

Step 1 – The user provides his/her username.

***Step 2* –** After the username is provided the user is asked to perform his 3D signature movement. The 3D signature characteristics are collected in order to be validated.

1. The data used for validation are:
2. Elapsed time for the completion of the gesture.
3. The gesture is divided in smaller equal duration parts (time slots) for which the maximum and minimum acceleration values per axis is collected.
4. Starting sensor position (pitch, roll values)
5. Ending sensor position (pitch, roll values)
6. Total maximum and minimum acceleration value per axis is collected.

This step can be repeated up to three times. If the process is completed correctly then proceed to ***Step 5.***

If all three attempts fail then proceed to ***Step 4*** or optionally ***Step 3***.

Step 3* –** Textual password is needed in order to authenticate the user. If this step fails once, proceed to ***Step 4, else proceed to ***Step 5.***

***Step 4* –** The user is banned and the account is suspended. Further actions can be taken that are out of the scope of this paper.

***Step 5* –** The user is successfully authenticated

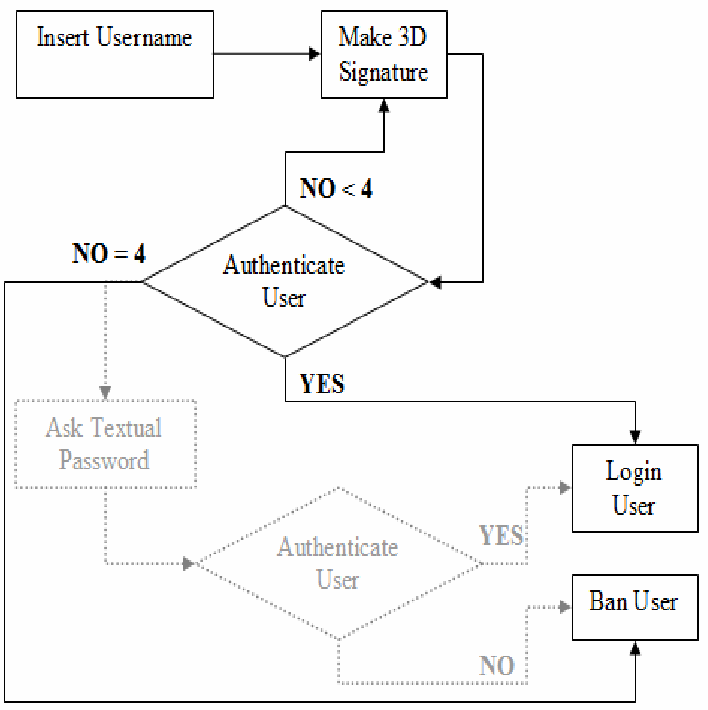


Fig. 2. User authentication process

4.3 Advantages

The advantages of the proposed authentication method are covering both practical and security issues.

Besides the fact that the proposed authentication method is innovative and intriguing for the user in relation to textual passwords, it has some other major advantages that must be pointed out, which are as follows:

1. The 3D signature password created is easier to remember than a "secure" 8 digit password.
2. The 3D signature password is faster and easier to perform than typing a secure 8 digit password.
3. The 3D signature password is difficult to steal; shoulder surfing attacks are difficult to succeed.

4. The 3D signature password cannot be written down, or given away to be performed by someone else.
5. It's cheaper to implement in many different devices (e.g. mobile phones), where biometrics would be difficult to implement.

5 User Authentication Implementation

In order to prove the validity of the proposed authentication method an implementation was designed, utilizing a simple commercial 3D accelerometer sensor and the use of a java library to capture acceleration data. The *WiiuseJ* [19] is an opensource java API which facilitates the use of *wii remote* on any computer.

5.1 Wii Remote

The *Wii Remote*, sometimes unofficially nicknamed "*Wiimote*", is the primary controller for Nintendo's Wii console. A main feature of the Wii Remote is its motion sensing capability, which allows the user to interact with and manipulate items on screen via gesture recognition and pointing through the use of accelerometer and optical sensor technology. The controller communicates wirelessly with the console or a personal computer via short-range Bluetooth radio, with which it is possible to operate up to 10 meters away from the console. The controller's symmetrical design allows it to be used in either hand. The Wii Remote has the ability to sense acceleration along three axes through the use of an ADXL330 accelerometer.

5.2 SquWiigle v1.0 Concept

SquWiiggle, derives from the word *squiggle* which means, a mark or movement in the form of a wavy line and the word *Wii* (Nintendo Game Console). While our prototype is based on the Wii remote hardware, the proposed authentication technique can be implemented to any device with a three-axis accelerometer similar to those found in most consumer electronics and mobile devices.

5.2.1 Implementation Specifications

The most important part of the implementation was the analysis of the 3D password gesture. In order to collect enough data to authenticate a user, different parameters must be stored:

Parameter 1: Elapsed time for signature completion

The elapsed time is the time duration between starting the capturing procedure of the 3D signature up to ending it. Time is calculated in milliseconds (ms)

Parameter 2: Maximum and minimum acceleration values per axis for segments

The 3D signature performed is divided in equal time segments. The number of segments depends on the elapsed time and is usually equal to:

$$\text{Segment Number} = 0.3 * \text{ElapsedTime(sec)}$$

For each segment the maximum and minimum acceleration values per axis (x, y, z) are calculated and stored.

Parameter 3: Starting sensor position

Starting sensor position is the position in which the user holds the acceleration sensor in order to start performing the password gesture.

The position can be described by the roll and pitch values that can be easily calculated using the following equations (1), (2).

$$\mathbf{roll} = \arctan2(a_z, a_x) \tag{1}$$

$$\mathbf{pitch} = \arctan2(a_z, a_y) \tag{2}$$

a_x = x axis acceleration, a_y = y axis acceleration, a_z = y axis acceleration

The *ArcTan2* function calculates ArcTan(Y/X), and returns an angle in the correct quadrant. The values of *X* and *Y* must be between -264 and 264. *X* can not be 0. The return value will fall in the range from -Pi to Pi radians.

Parameter 4: Ending sensor position

Ending sensor position is the position in which the user holds the acceleration sensor when he has finished performing the password gesture.

The position can be described by the roll and pitch values that can be easily calculated using the equations (1), (2).

Parameter 5: Total maximum and minimum acceleration value per axis

The total maximum and minimum acceleration per axis is calculated by simple storing the biggest and the smallest value per axis calculated on step 2.

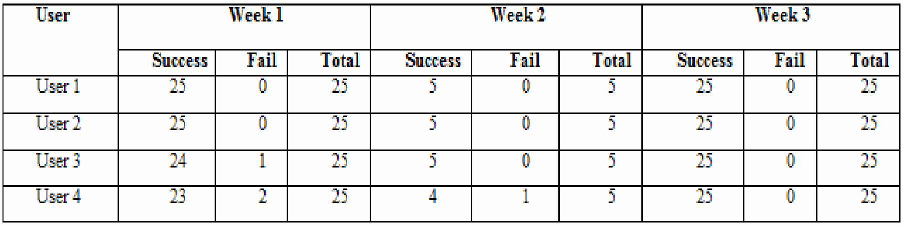
6 Security Tests and Results

The Security tests where designed in order to prove both the validity of the proposed authentication method and the robustness of the algorithm in security attacks. The four users where divided in two categories experienced and inexperienced of different ages ranging from 16 to 51 years of age.

In the first test performed, the users had to register themselves in the system and then authenticate themselves for a three weeks period.

The following table depicts the authentication results along with failed attempts over time. The success rate is high with an average of 98.2% of successful authentication.

Table 1. User Authentication Attempts Results



User	Week 1			Week 2			Week 3		
	Success	Fail	Total	Success	Fail	Total	Success	Fail	Total
User 1	25	0	25	5	0	5	25	0	25
User 2	25	0	25	5	0	5	25	0	25
User 3	24	1	25	5	0	5	25	0	25
User 4	23	2	25	4	1	5	25	0	25

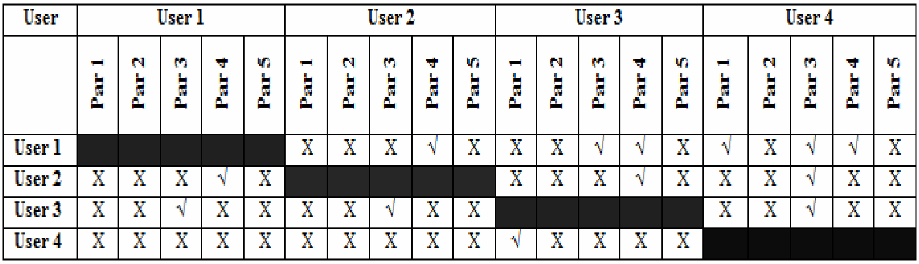
The following table depicts the time needed for each process along with the equivalent time for textual authentication using a strong 8 digit password for the first time. The 3D signature registration process is relatively slower than textual, but the authentication process is faster. Results were retrieved after ten attempts per user.

Table 2. User Registration – Authentication Timing

User	**3D Signature, Registration**	**Textual Password, Registration**	**3D Signature, Authentication**	**Textual Password, Authentication**
User 1	35 sec	29 sec	6 sec	6 sec
User 2	39 sec	30 sec	6 sec	7 sec
User 3	49 sec	55 sec	7 sec	10 sec
User 4	55 sec	58 sec	9 sec	12 sec

In order to test the security robustness of the proposed authentication algorithm we performed our secret gestures publicly in order for other users to try them for us, as a form of shoulder surfing attack. The following results indicate why the rest of the users could not imitate our private 3D gesture password. No unauthorized user could use our 3D signature in order to authenticate himself on behalf of us.

Table 3. Shoulder surfing attacks results for five authentication parameters, (X: fail, √: success)



User	User 1					User 2					User 3					User 4				
	Par 1	Par 2	Par 3	Par 4	Par 5	Par 1	Par 2	Par 3	Par 4	Par 5	Par 1	Par 2	Par 3	Par 4	Par 5	Par 1	Par 2	Par 3	Par 4	Par 5
User 1	■	■	■	■	■	X	X	X	√	X	X	X	√	√	X	√	X	√	√	X
User 2	X	X	X	√	X	■	■	■	■	■	X	X	X	√	X	X	X	√	X	X
User 3	X	X	√	X	X	X	X	√	X	X	■	■	■	■	■	X	X	√	X	X
User 4	X	X	X	X	X	X	X	X	X	X	√	X	X	X	X	■	■	■	■	■

With the help of this test interesting conclusions where made as far as which parameter of the authentication algorithm was more prone to attacks. The starting sensor position (*Parameter 3*) and ending sensor position (*Parameter 4*) where imitated in more than one occasions by unauthorized user, while non static parameters in terms of motion were not imitated due to lack of muscle memory. Elapsed time for signature completion (*Parameter 1*) was also imitated more than one occasion as it can be easily calculated. Although parts of the authentication algorithm were imitated by unauthorized users the algorithm can be considered robust to shoulder surfing attacks in comparison to textual authentication techniques which would have surely failed.

7 (Re)-Usability Tests and Results

The (Re)-Usability tests where designed in order to prove that the proposed authentication method can be user friendly and at the same time provide a sufficient substitute for textual passwords but without their drawbacks. Great effort was made in order to prove that user can remember a 3D password after a sufficient period of time and tested the results against a strong 8 digit textual password.

In the first test the users chose a never used before 3D password and a strong textual password. They authenticated themselves one time per day for five days in a row. After that period they stopped using their passwords for two weeks and then were asked to authenticate once more.

The results on *Table 4* depict a slightly better hit ratio when using a 3D password.

Table 4. Easier to remember, (X: no, √: yes)

User	3D Signature	Textual Password
User 1	√	√
User 2	√	√
User 3	√	X
User 4	X	X

8 Conclusions and Future Work

In this paper, we have proposed a unique user authentication technique based on gesture recognition and a tri-axis accelerometer and presented basic usability results thought our SquWiigle implementation. With the proliferation of low power, low cost accelerometers, we believe that accelerometer and gesture-based user authentication has the potential to enable personalized services on resource constrained mobile devices, and to that direction we are investigating a variety of applications such us mobile payments, serious games and in gaming in general. Considering existing open research issues, we believe that further feature analysis of 3D axis acceleration along with more sophisticated solutions in handwritten signature forensics, and adaptive solutions to personalize the rejection threshold can help achieve more effective and usable gesture-based authentication. To this direction we are planning a thorough series of experiments with more users evaluating the proposed method in order to get safer results considering the usability and robustness of the method.

References

1. Haghighi, A.P., McCabe, B.D., Fetter, R.D., Palmer, J.E., Hom, S., Goodman, C.S.: Retrograde control of synaptic transmission by postsynaptic CaMKII at the Drosophila neuromuscular junction. Neuron 39, 255–267 (2003)
2. McCabe, B.D., Marques, G., Haghighi, A.P., Fetter, R.D., Crotty, M.L., Haerry, T.E., Goodman, C.S., O'Connor, M.B.: The BMP homolog Gbb provides a retrograde signal that regulates synaptic growth at the Drosophila neuromuscular junction. Neuron 39, 241–254 (2003)
3. Muscle Memory, Dow 207 (1), 11, Journal of Experimental Biology, `http://jeb.biologists.org/cgi/content/full/207/1/11`

4. Osborn, A.S.: Questioned Documents, 2nd edn. Boyd Printing Company, New York (1929) (Reprinted Nelson-Hall Co., Chicago)
5. Liu, J., Wang, Z., Zhong, L., Wickramasuriya, J., Vasudevan, V.: uWave: Accelerometer-based Personalized Gesture Recognition and Its Applications. In: Proc. IEEE Int. Conf. Pervasive Computing and Communication, PerCom (2009)
6. Hofmann, F.G., Heyer, P., Hommel, G.: Velocity Profile Based Recognition of Dynamic Gestures with Discrete Hidden Markov Models. In: Proc. Int. Wrkshp. Gesture and Sign Language in Human-Computer Interaction (1997)
7. Jang, I.J., Park, W.B.: Signal Processing of the Accelerometer for Gesture Awareness on Handheld Devices. In: Park, W.B. (ed.) Proc. IEEE Int. Wkshp. Robot and Human Interactive Communication, pp. 139–144 (2003)
8. Kela, J., Korpipää, P., Mäntyjärvi, J., Kallio, S., Savino, G., Jozzo, L., Marca, D.: Accelerometer-based gesture control for a design environment. Personal Ubiquitous Computing 10, 285–299 (2006)
9. Payne, B.D., Edwards, W.K.: A Brief Introduction to Usable Security. IEEE Internet Computing 12, 13–21 (2008)
10. Maltoni, D.: Handbook of fingerprint recognition. Springer, Heidelberg (2003)
11. Zhao, W., Chellappa, R., Phillips, P.J., Rosenfeld, A.: Face recognition: A literature survey. ACM Computing Surveys 35, 399–458 (2003)
12. Wildes, R.P.: Iris Recognition: an Emerging Biometric Technology. Proc. IEEE 85, 1348–1363 (1997)
13. Campbell Jr., J.P.: Speaker Recognition: a Tutorial. Proc. of the IEEE 85, 1437–1462 (1997)
14. Impedovo, D., Pirlo, G.: Automatic signature verification: the state of the art. IEEE Trans. on Systems, Man, and Cybernetics, Part C: Applications and Reviews 38, 609–635 (2008)
15. Okumura, F., Kubota, A., Hatori, Y., Matsuo, K., Hashimoto, M., Koike, A.: A Study on Biometric Authentication Based on Arm Sweep Action with Acceleration Sensor. In: Proc. Int. Symp. Intelligent Signal Processing and Communications (2006)
16. Farella, E., O'Modhrain, S., Benini, L., Riccó, B.: Gesture Signature for Ambient Intelligence Applications: A Feasibility Study. In: Fishkin, K.P., Schiele, B., Nixon, P., Quigley, A. (eds.) PERVASIVE 2006. LNCS, vol. 3968, pp. 288–304. Springer, Heidelberg (2006)
17. Matsuo, K., Okumura, F., Hashimoto, M., Sakazawa, S., Hatori, Y.: Arm Swing Identification Method with Template Update for Long Term Stability. In: Proc. Int. Biometrics (2007)
18. Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S.M., Ailisto, H.A.: Identifying Users of Portable Devices from Gait Pattern with Accelerometers. In: Proc. of IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP), vol. 2, pp. ii/973–ii/976 (2005)
19. Duche, G., Wiiuse, J.: `http://code.google.com/p/wiiusej/`

A Correlation Approach to Intrusion Detection

Massimo Ficco[1] and Luigi Romano[2]

[1] Dipartimento per le Tecnologie, Universita' degli Studi di Napoli "Parthenope"
Centro Direzionale di Napoli, IT
[2] Laboratorio ITeM, Consorzio Interuniversitario Nazionale per l'Informatica (CINI)
Via Cinthia - Edificio 1, 80126 Napoli, IT
massimo.ficco@consorzio-cini.it,
luigi.romano@uniparthenope.it

Abstract. In this paper we discuss the limitations of current Intrusion Detection System technology, and propose a hierarchical event correlation approach to overcome such limitations. The proposed solution allows to detect attack scenarios by collecting diverse information at several architectural levels, using distributed security probes, which is then used to perform complex event correlation of intrusion symptoms. The escalation process from intrusion symptoms to the identified target and cause of the intrusion is driven by an ontology.

Keywords: detection, fusion, correlation.

1 Introduction

In the last years, Intrusion Detection System (IDS) has emerged as the main technology to protect information systems. The IDSs do not directly detect intrusions, but only the attacks symptoms. Different works [1,2] have observed that IDSs can generate thousands of alerts per days, up to 99% of which are false positives, that make it very difficult to identify the real attacks in progress over the system.

The intrusion detection methods can be divided into two categories: misuse- and anomaly-based [3]. Anomaly detection consists in comparing the observed beaviour with a reference "expected" beaviour. Any deviation between the two beaviours triggers an alarm. Misuse detection solutions consist of comparing the observed beaviour with a reference defining known attack sets. Both types of detection methods are characterized by a number of false positives and false negatives [4]. Misuse detection methods have the advantage of identifying specific attacks, with a few false positives. However, they only enable the detection of symptoms of known attacks forcing the security administrators to regularly update their signature sets. On the other hand, the anomaly-based solutions present the advantage of a great generalization capability, which leads to the ability of detecting new attacks. A major drawback is that no evidence is provided about the root cause of the monitored anomaly (*i.e.*, the reason for which it occurs): (*i*) no diagnosis is performed in order to help the administrator to

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 203–215, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

identify whether an alert is a false positive or not; and (*ii*) in the case of a true positive, no information is provided about the attack that has led to the anomaly [5]. Finally, none of the two methods provides any support to recognize complex attack scenarios, *i.e.*, mechanisms to understand the relationship among sequence of different attacks [6].

In order to overcome the above mentioned limitations, in this paper we propose a solution, which exploits a hierarchical event correlation process based on diversity both in information sources and methods used to detect malicious activities. Different detection methods are adopted to collect streams of information at several architectural levels (*i.e.*, network, operating system, data base, and application), using multiple security probes, which are deployed as a distributed architecture. In order to increase the detection coverage and reduce the time and the cost of managing the large number of false positives generated by probes, a "*clustering*" correlation approach is adopted to aggregate attack symptoms (based on similarity among symptoms attributes [7]), and rearranging the resulting alarms based on their confidence levels [8]. The confidence indicates the likelihood that the correlated alarms are symptomatic of an ongoing attack on the system. It is estimated on the base of "weights" and "thresholds" that provide points of operation that offer the best compromise between the false positives and false negatives. In order to recognize complex attack patterns and enrich the semantics of alerts, a "*causal*" correlation approach is adopted, which captures the causal relationships among the resulting alarms (which can represent intermediate attacks of a more complex attack scenario), by correlating them on the base of temporal and logical constraints [9]. The correlation capability is driven by an ontology (specified in OWL). It is used to recognize attack scenarios and to identify the cause of the symptoms, which are discovered.

Finally, we show that the proposed solution is able to detect both attacks that are characterized by a single malicious activity, called intermediate attacks (*e.g.*, SQL injection), and complex attacks that consist of a specific sequence of malicious activities perpetrated by the attackers in order to discover system's vulnerabilities. We conducted two sets of preliminary experiments on a testbed consisting of web servers running different well known open source content management systems. The former set of experiments exposed the most serious vulnerabilities [10] of the web applications, which are described in the Bugtraq repositories. By using a complex event processing technology, that correlates different alarms on the base of temporal and logical conditions, the latter experiments show the capabilities of the proposed solution to recognize attack scenarios on the fly, as they occur. The experimental tests have shown that our approach results in a better performance of the IDS, in terms of reducing the false positive alarms rate and increasing detection capacity, as well as more accurate identification of the nature of the attack and the specific system component affected by it.

2 Related Work

In order to improve the attack detection rate, enrich the semantics of alarms, and reduce the overall number of false alarms, different works propose explicit

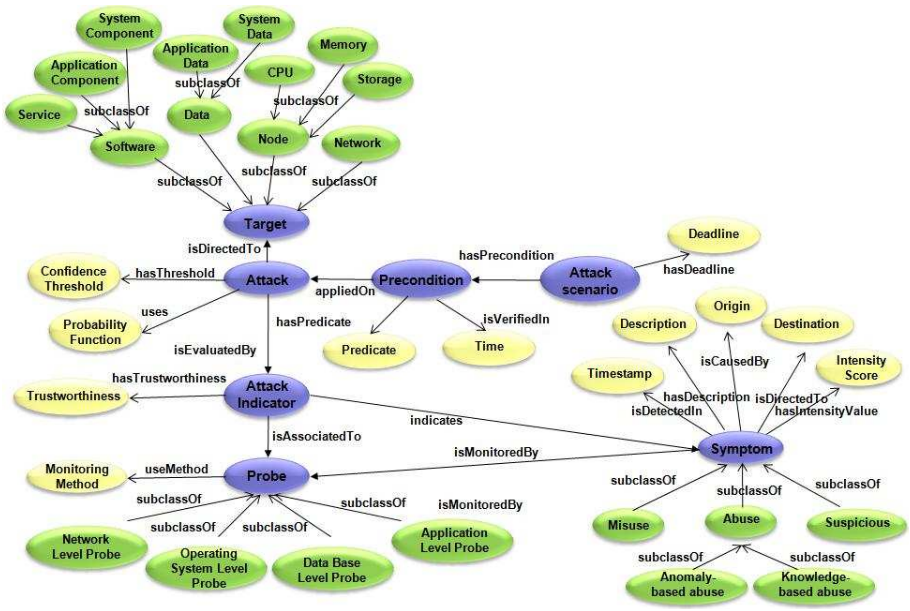


Fig. 1. A simplified view of the proposed ontology

alarm correlation approaches. In particular, Valeur et *al*. [11] proposes a correlation workflow intended to unify the various steps of the correlation process. Our work is strongly inspired by the this framework, but we propose a weight-based correlation approach, in which each monitored symptom is weighted on the base of the trustworthiness of a probe to monitor a specific attack. Majarczyk et *al*. [12] propose an intrusion detection architecture based on COTS diversification applied to Web applications. The authors adopt an approach for anomaly detection using redundancy and diversification techniques. Although, the proposed solution provides a high attacks detection, and a low level of false positives, no diagnostic function is defined in the system. Moreover, they have only restricted experiments to the contents of static http requests/responses. Both Haibin et *al*. [13] and [12] adopt correlation approaches that combine only events that represent the independent detection of the same attack occurrence by different probes. They have not proposed any mechanism for the recognition of attack scenarios. Morin et *al*. [9] proposed a misuse correlation approach based on the chronicles formalism, which is a high level declarative language to describe temporal patterns that represent possible evolutions of attack scenarios. On the other hand, the use of raw security data (attack's symptoms) in the correlation process, implies the need to define a large number of correlation signatures computationally complex to perform. In our work, symptoms are before aggregate in high-level messages, which represent intermediate attacks, and then they are correlated to recognize the attack scenario.

3 Ontology-Based Approach

The proposed ontology drives the correlation process in order to recognize more complex attack scenarios, as well as to aggregate symptoms produced by different probes with the final goal of identifying one or more intermediate attacks as likely causes of observed symptoms. Ontology is also used to automate the process of deriving queries for diagnostic analysis. Figure 1 presents a simplified view of our security ontology, which is implemented in Web Ontology Language (OWL). Each kind of attack can be related to a set of potential symptoms. More specifically, an attack is described by using *attack indicator*, that estimates the trustworthiness of the probe to detect the specific symptom. *AttackIndicator* has the properties: (*i*) *hasTrustworthinessValue*, which is defined by the concept of likelihood that the observed feature is a symptom of the considered attack, (*ii*) *isAssociatedTo*, which is defined by the concept *Probe*, and (*iii*) *indicates*, which is defined by the concept *Symptom. Symptoms* are classified into Abuses, Misuses and Suspicious Acts. *Abuses* represent actions which change the state of a system's asset. They are further divided into *Anomaly-* and *Knowledge-based.* The former represents anomalous behaviors (*e.g.*, unusual application load, anomalous input requests), whereas the latter is based on the recognition of signatures of previously known attacks (*e.g.*, brute force attacks). *Misuses* represent out-of-policy behaviors in which the state of the components are not affected (*e.g.*, authentication or queries failed). *Suspicious Acts* are not violations of policy, but events of interest to the system administrator (*e.g.*, commands providing information about the system state). Each *Symptom* is characterized by the property *hasIntensityScore*, which reflects the probability of occurrence of the given symptom with regards to the specific monitoring method. *Probes* are characterized by *Monitoring Method* property, which defines the method used to monitor the symptom. Moreover, they are also classified depending on the specific architectural level to which they belong, namely *Network Level Probe*, *Operating System Level Probe*, *Data Base Level Probe* and *Application Level Probe.* A similar classification is adopted for *Target*, that refers to anything that should be protected: *Network*, *Node*, *Data* and *Software.* Finally, *Attack Scenario* identifies the correlation rule for the attack scenario recognition. It has proprieties *hasDeadline* and *hasPrecondition.* The former defines the time window by which monitoring the attack scenario. The latter defines the *Precondition*, which describes the conditions required for including an intermediate attack in the considered scenario. The *Precondition* has the properties: *Time*, which is the temporal condition for attack detection of an intermediate attack, and *Predicate*, which corresponds to a numerical or logical condition over the attack instance to be verified.

4 The Detection and Diagnosis Process

The proposed process produces a diagnostic report that shows what parts of the system are under attack, and what kind of attacks the system is experiencing. In the following, the steps performed by the process are described.

- **Monitoring:** Distributed probes observe different attack symptoms by using specific monitoring methods. For each symptom, the method computes a probability value, named *Intensity Score* (IS), which reflects the likelihood that the observed symptom represents a malicious behavior.
- **Classification:** Symptoms are analyzed, filtered and aggregated in categories. Symptoms are classified on the base of the concepts presented in the proposed ontology (*i.e.*, misuses, anomaly-based, knowledge-based, and suspicious acts).
- **Normalization:** Since each probe can provide security information with different representations or formats, every monitored symptom is coded and normalized in a standardized format, as well as augmented with additional information, such as timestamp, probe identifier, source and target of the monitored anomalous behavior.
- **Fusion:** It receives the classified symptoms and aggregates them by using *clustering-based* correlation rules. They combine symptoms based on the 'similarity' among their attributes. In this work we consider aggregation based on the attack type, the target component, and the temporal proximity, *i.e.*, we combine different symptoms of the same attack occurrences, which are directed to the same target. For each monitored target, the ontology identifies the symptoms to aggregate for each potential attack associated with that target. The temporal proximity is based on a time window Tc, that is specified as a parameter by the administrator. We are aware that a temporal order requires that all clocks at probes be synchronized. We do not address this issue here, since this problem is out of scope of this work. Several approaches can be used, *e.g.*, using a total ordering based on timestamps. At the end of this phase, for each target, an event $E(k) = \{e_{A1}(k), ..., e_{Am}(k)\}$ is generated. For each possible attack A_i, $e_{Ai}(k)$ contains the symptoms correlated during the time window k.
- **Ranking and filtering:** In order to reduce the number of false positives produced during the fusion step, we adopt an approach based on the *confidence* (C) of the events. Assuming that $e_{Ai}(k) = \{s_1, ..., s_z\}$ is the set of correlated symptoms related with the attack of type Ai during the time window k, the confidence is the likelihood that the monitored symptoms represent an underlining attack of such a type. C_{Ai} is computed using Function 1.

$$C_{Ai}(k) = \sum_{s \in e_{Ai}(k)} \omega_p(s) * IS_s(k) \quad with \;\; \omega_p \leq 1 \tag{1}$$

The confidence C_{Ai} depends on the weights ω_p and the intensity scores ISs of the correlated symptoms. Then the observed features ISs are normalized to zero mean and unit variance. $\omega_p(s)$ is associated with trustworthiness of the probe p to monitor a symptom of the attack Ai. It is assigned on the base of a prior knowledge of the effectiveness of monitoring method being used for the given attack type. Although simple in implementation, choosing proper weights is of critical importance to highlighting the proper features under various attacks. A mapping function normalizes the calculated C_{Ai} values into a value on a scale of 0 to 255. The events ordered on the base of the C_{Ai}

given an indication of most likely cause of detected anomalous behaviors at the step k (intermediate attacks). Finally, the events are subjected to a filtering. If the confidence does not exceed a threshold (specific of each attack) estimated during a validation phase, the event will be discarded (*i.e.*, it is considered as a false positive).

- **Correlation:** The goal of the correlation is to identify complex attack scenarios. In the intrusion detection literature, attack scenario (or attack pattern) is a sequence of explicit attack steps (intermediate attacks), which are logically linked and lead to an objective. In our work, an attack scenario is modeled by a *causal-based* correlation rule. It consists of a set of preconditions, which are logical conditions on the intermediate attack alarms (IAA). Preconditions are linked together by temporal constraints. Each precondition is described by predicates, which are conditions to be verified (*e.g.*, the number of IAAs of type Ai must be greater than 5). A deadline is fixed for the recognition of each scenario. The IAAs can be shared by many attack scenarios. The integration of an IAA A_i in an attack pattern recognition depends on the IAA's timestamp t_i, the previously integrated IAAs, and the predicates p_i. An instance of an attack scenario can be described by the following representation:

```
Attack scenario {
    alarm(A1,t1,p1.1,p1.2,p1.3,...);
    alarm(A2,t2,p2.1,p2.2,...);
    alarm(A3,t3,p3.1,...);
    alarm(A4,t4,p4.1,...);
    t1<t2<t3<t4;
    t4-t1 < deadline; }
```

  During the recognition process many partial instances of attack scenarios must be managed. If a predicate is violated, or if a deadline expires, then the instance is dropped, and their constitutive IAA are either correlated to other scenarios or provided to the administrator individually. When a complete match is found, an attack scenario instance is recognized and an alarm is triggered.
- **Diagnosis:** If an attack scenario instance is recognized, a compact report is built and shown to the administrator. This report is hierarchically structured. The leaf nodes are the symptoms monitored by probes, and the root nodes are the higher level alarms (related to an attack scenario). The intermediate nodes represent IAAs. For each IAA, the report contains a summary of the information produced during the previous phases, including the attack type, the confidence, and the target of the attack. Only the hierarchies root are directly shown to the administrator (*i.e.*, the symbolic name of the recognized scenario, and the final target of the attack). If detailed information about the alarms are required, the administrator can browse the alarms hierarchy. Such a recognition process contributes to alarm volume reduction since only one alarm (the recognized scenario) is provided to the administrator instead of each individual alarm (*i.e.*, the intermediate attack). However,

as described in [9], not all attacks can be modeled using scenarios. Firstly, the relevance of an attack scenario is questionable, because many (unpredictable) pattern may lead to a given attack objective. Secondly, it is hard to specify quantitative time constraints in scenarios, because the time gaps among each step may vary a lot, depending on how hurried the attacker is. Moreover, attack can simply consist of a single malicious action (*e.g.*, a single SQL injection attempt). Therefore, alarms that cannot be merged to any scenario, are provided to the administrator individually and rearranged on the base of their confidence levels.

5 Case Study, Experimental Setup and Results

In this section, we present preliminary results obtained by applying the proposed approach in a laboratory experimental setup. In a first set of experiments, we present an example of the detection and diagnosis process of an intermediate attack. It shows that the aggregation of information collected at several architectural levels, using multiple security probes, allows to improve the detection capability and reduce false positives. In a second set, we present an example of attack pattern recognition. The experimental setup consist of the most well-known open source content management systems written in PHP, including Joombla (v.1.5), phpNuke (v.6.0, v.7.1), Mambo (v.4.5), and Drupal (v.4.7). They run on an Apache v1.3.34 web server, and use PHP v4.4.2 and MySQL v4.1.11.

5.1 Detection and Diagnosis of Intermediate Attacks

In order to validate the proposed process, we consider two classes of attacks: SQL Injection Attacks (SQLIA) and Cross Site Scripting (XSS). They are the most frequent (and most serious) classes of attacks for web applications [10]. For the considered applications, such vulnerabilities are described in the SecurityFocus advisories with Bugtraq IDs 10749, 10741, 15421, 9879, 3609, 13966, 26735, as well as in the Secunia Advisories Bugtraq IDs SA30461, SA31126, SA30922, SA21859, SA10413.

Monitoring and fusion. In order to monitor the attack symptoms we use different probes, which use either anomaly detection methods (AD) or misuse detection methods (MD). In AD methods a value (*Intensity Score*) is assigned to the generated events, which reflects the intensity of the given anomaly with regard to an established profile. For each observed feature, the AD approach can perform in one of three phases: training, validation, and testing. In the training phase data sets are used to parameterize the monitoring method (necessary to determine the characteristics of ‘expected’ beaviour). The suspicious requests are manually extracted in order to guarantee that the data sets are (as much as possible) attacks free. These requests are used during the testing phase to evaluate the used method. The validation phase aims at validating the detection models and to establish thresholds, that are used to distinguish between regular and anomalous behaviors during the testing phase. In the testing phase the AD

method is used to monitor anomaly behaviors with respect to the desidered profile computed during the training phase. The choice of a proper threshold value is the main problem in this process, since there is a trade-off between the number of false positives and the expected detection accuracy: a low threshold can result in many false positives, whereas a high threshold can result in many false negatives. Once the profiles and thresholds have been derived, the testing phase is operated. If the computed intensity score exceeds the fixed threshold a message is triggered. As for MD methods, since they also produce false positives, the intensity score of the generated messages is fixed to a value from 0 to 1. It is estimated during a validation phase, and represents the likelihood to monitor correctly an attack symptom. Table 1 shows the adopted probes, the relevant monitored features during the attacks, the related information sources, and the models/methods used to monitor symptoms.

Table 1. Features evaluated

Probe	Observed featurs	Source	Method/Model
AD-CD	Character distribution	HTTP traffic	AD: Chi-Square test
AD-QL	Query request length	HTTP traffic	AD: Chebyshev inequality
MD-QF	Query failed	Data base log	MD: Pattern recognition
AD-WR	Web response length	Web server log	AD: Chebyshev inequality
MD-SM	Signature of the HTTP request	HTTP traffic	MD: Signature matching
MD-TM	Content of the request	HTTP traffic	MD: Tag matching
AD-QS	Query syntax	Data base log	AD: Model-based

We briefly describe the considered features and the models adopted to perform the monitoring methods. The first four methods are *AD* methods detail described in our previous work [15].

- *Character Distribution (AD-CD)*: It is a method used to capture the concept of 'normal' query's attributes contained in the GET and POST HTTP request sections (*i.e.*, identifies anomalous character distribution). It is based on the *chi-square* function.
- *Query Length (AD-QL)*: It adopts a *Chebyshev Inequality* function to estimate an approximation of the actual distribution of the query's attributes length and detects suspicious inputs that significantly deviate from the observed normal behavior.
- *Queries Failed (MD-QF)*: During a time slicing window, it estimates abnormal rate of queries failed with respect to the normal operational model. In the validation phase, for each database table is fixed a threshold failures rate.
- *Web Response (AD-WR)*: It is based on a model similar to the one used for AD-QL monitoring in order to detect anomalous size of the page generated against the same request.
- *Signature Matching (MD-SM)*: It examines HTTP requests and determines whether a signature of previously know attacks is matched. It is based on Scalp IDS [16].

- *Tag Matching (MD-TM)*: It simply looks for trivial script tags present in the GET and POST HTTP request sections, such as “<script>”, “<img scr=”, “<b>”, “<u>”. Moreover, it monitors specific meta-characters, and injected string such as ‘union’, ‘insert’, 1’or‘1’=‘1 and their hexadecimal equivalents.
- *Query Syntax (AD-QS)*: It performs a syntax-aware evaluation of the query string before it is executed, similar to that proposed by [10]. It is a model-based approach used to identify anomalous queries that might be associated with an attack. The query string is parsed to break the string into a sequence of tokens that correspond to SQL keywords, operators, and literals. Then an iteration process checks whether tokens contain trusted data. If all tokens do not pass this check, the query is considered unsafe.

The evaluation of the proposed approach was performed using different data sets from production servers at the university in which the considered applications run. During the training phase, we considered the legitimate requests of three months of real traffic. A validation set is used to validate the models, and to estimate thresholds. For each application, during the testing phase we created a synthetic data set in which a number of attacks (collected on the web), their obfuscated variations (using hexadecimal characters) and normal requests (the traffic of the last month) were introduced. For each application, Table 5.1 shows the total number of normal HTTP query requests and the illegitimate requests (injected during the testing phase by Apache Jmeter [17].

Table 2. Requests for considerate data sets

Applications	Legitimate Requests	Illegitimate Requests	
		SQLIA	XSS
Joomla	372.732	45	24
phpNuke	201.318	36	16
Mambo	129.786	27	21
Drupal	545.760	41	14
Total	**1.249.596**	**149**	**75**

Experimental evaluation. For each possible attack to the monitored target, the fusion step aggregates symptoms on the base of the schema defined by the ontology and their temporal proximity. Figure 2 shows the monitoring and fusion results of the XSS and SQLIA attacks. For each method, the percentage of detected attacks (DAs), and the number of requests that have been classified as false positives (FPs) are provided. These results represent the capacity of each method to monitor potentially malicious behaviors compared with the fusion process results. Results show that each method does not achieve a detection rate of 100%, and presents many false alarms. For example, the AD-WR method presents the highest number of FPs, whereas AD-CD presents the highest rate of detected attacks. MD-TM produces the lower rate of false positives.

As one might expect, the use of multiple probes in the fusion process increases the number of FPs (about 18% compared to AD-WR). On the other hand, the percentage of DAs is increased (100% for SQLIA and 98% for XSS).

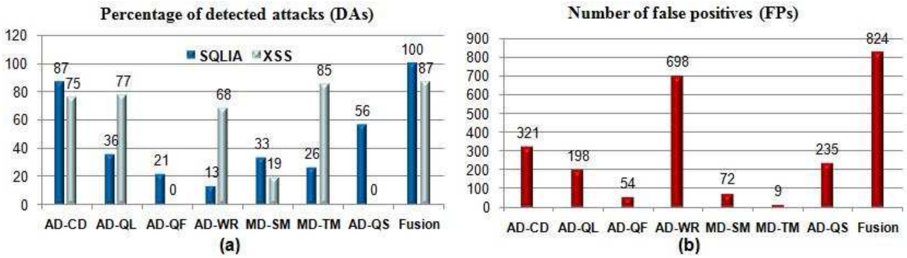


Fig. 2. Fusin process results

Ranking and diagnosis. After fusion, the resulting alarms are ordered based on their confidence C_{Ai}. If the estimated confidence value exceeds a fixed threshold C_T, an IAA alarm is triggered. C_{Ai} is computed using Function 1 with a time window equal to two minutes and $n = 1$ (for each method). For each attack, Table 3 shows the levels of trustworthiness ω_p of the probes inferred during the validation phase. We considered five levels: NULL (0.0), VERY LOW (0.1), LOW (0.3), MEDIUM (0.5), HIGH (0.7) and VERY HIGH (0.9). Figure 3 reports the number of DAs and FPs with respect to the confidence values. It can be noted that by choosing a confidence threshold value C_T of 75, it is possible to reduce the FPs rate of about 98% (*e.g.*, events that are not correlated with other events, or present low intensity scores), while leaving the number of DAs unaffected (only 2% reduction). In order to evaluate the ability of our approach to detect and classify alarms (diagnosis capability), two traditional indexes are considered: recall and precision. *Recall* represents the likelihood that a specific

Table 3. Probes trustworthiness

Probes	**Trustworthiness**	
	SQLIA	**XSS**
AD-CD	HIGH	MEDIUM
AD-QL	LOW	HIGH
MD-QF	HIGH	NULL
AD-WR	VERY LOW	MEDIUM
MD-SM	HIGH	MEDIUM
MD-TM	LOW	VERY HIGH
AD-QS	HIGH	NULL

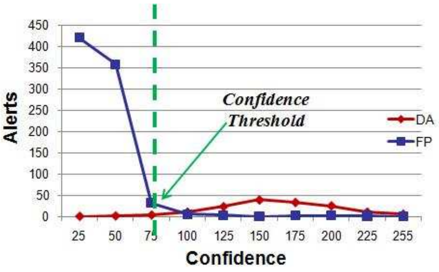


Fig. 3. Monitoring and ranking results

Table 4. The considered complex attack scenario

Attack/ Symptom	Description
Port scanning	A scanning procedure is adopted to trace the open ports on the considered server (*e.g.*, the port 80, 21, 22, 8080 and 3120 are discovered).
Telnet	The discovered port 80 is used to determine if a web server is listening on that port (*e.g.*, by a telnet request)
Directory traversal	By sending to the Apache server a custom request, consisting of a long path name created artificially by using numerous *dot-dot-slash*, the attacker gains a listing of the web server directory contents. During this step, a hidden web page (no public link to that page is published on the web) is discovered.
Policy violation & Buffer overflow	The attacker enters strings (*e.g.*, login data) with variable length as GET parameters. With very long strings an error message is displayed within the Web page. The page contains the login query performed in the data base.
SQL injection	Known the query structure (in terms of tables in which are located login information), the attacker performs attacks by POST requests.

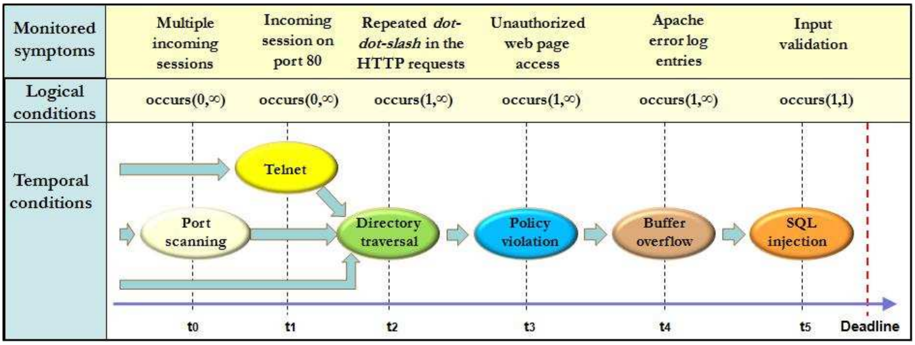


Fig. 4. The attack preconditions set

attack is correctly diagnosed (*i.e.*, the number of correctly diagnosed attacks Ai over the number of total injected attacks of such a type), while *precision* represents the likelihood that an alarm tagged as a detected attack is really an attack. As we presented in Table 3, different monitored features can be considered symptoms of both XSS and SQLIA attacks, but with different trustworthiness values. Thus, the experimental results show that, considering only alarms with a level of confidence greater then 75, the percentage of SQLIAs correctly diagnosed was about 93% of injected attacks (5% attacks are marked as XSS), whereas the percentage of XSS was about 88% (9% attacks are marked as SQLIA). Moreover, considering the same confidence threshold, our approach presents a precision equal to 94%.

5.2 Attack Scenario Recognition

During an attack scenario, it is more likely that the attacker first performs the knowledge gathering steps, which consist of a set of commands that enable him/her to gain knowledge about the target system, and then performs the intrusion. For example, in Table 1, we describe an attack instance, which consists of a sequence of steps (intermediate attacks) followed by an attacker to discover and exploit a SQLIA vulnerability.

As graphically shown in Figure 4, the considered attack scenario can be modeled by a set of preconditions. They are specified by logical and temporal conditions (predicates), which are combined by using logical connectives (conjunctions and negations) among them. The presented set of preconditions can be coded in a complex query to be processed by a Complex Event Processor (CEP), such as [18,19]. In the current implementation we used Borealis [20].

6 Conclusions

In this work, we have discussed the limitations of current IDS technology, and proposed a hierarchical event correlation to overcome such limitations. We have conducted preliminary experiments on a testbed consisting of web servers running well known open source applications. The experimental tests have demonstrated that the use of a hierarchical correlation of different information: *i*) strengthens the diagnosis, *ii*) reduces the overall number of alarms, *iii*) improves the semantic content of the alarms, and *iv*) allows to detect attack scenarios. In future work, we will aim to define mechanisms for unknown attack patterns identification.

Acknowledgment

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 225553 (INSPIRE Project).

References

1. Axelsson, S.: The base-rate fallacy and the difficulty of intrusion detection. ACM Trans. on Information and System Security 3(3), 186–205 (2000)
2. Manganaris, S., Christensen, M., Hermiz, K.: A data mining analysis of RTID alarms. Computer Networks 34(4), 571–577 (2000)
3. Hervé, D., Dacier, M.: Towards a taxonomy of intrusion-detection systems. The Journal of Computer and Telecommunications Networking 9, 805–822 (1999)
4. Kemmerer, R., Vigna, G.: Intrusion detection: a brief history and overview. IEEE Computer 35(4), 27–30 (2002)
5. Majorczyk, F., Totel, E., Mé, L.: Anomaly Detection with Diagnosis in Diversified Systems using Information Flow Graphs. In: IFIP International Federation for Information Processing. LNCS, vol. 278, pp. 301–315. Springer, Boston (2008)
6. Ning, P., Cui, Y., Xu, D.: Techniques and tools for analyzing intrusion alerts. ACM Trans. on Information and System Security 7(2), 274–318 (2004)
7. Julisch, K.: Clustering intrusion detection alarms to support root cause analysis. ACM Trans. on Information and System Security 6(4), 443–471 (2003)
8. Yu, D., Frincke, D.: Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory. In: Proc. of the 43rd ACM Southeast Regional Conference, vol. 2, pp. 142–147 (May 2005)

9. Morin, B., Debar, H.: Correlation of intrusion symptoms: An application of chronicles. In: Vigna, G., Krügel, C., Jonsson, E. (eds.) RAID 2003. LNCS, vol. 2820, pp. 94–112. Springer, Heidelberg (2003)
10. The OWASP Top 10 Web attacks (December 2009), `http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project`
11. Valeur, F., Vigna, G., Kruegel, C.: A Comprehensive Approach to Intrusion Detection Alert Correlation. IEEE Transactions on Dependable and Secure Computing 1(3), 146–169 (2004)
12. Totel, E., Majorczyk, F., Mé, L.: COTS Diversity Based Intrusion Detection and Application to Web Servers. In: Valdes, A., Zamboni, D. (eds.) RAID 2005. LNCS, vol. 3858, pp. 43–62. Springer, Heidelberg (2006)
13. Haibin, M., Jian, G.: Intrusion Alert Correlation based on D-S Evidence Theory. In: Proc. of the 2th Int. Conf. on Communications and Networking (CHINACOM 2007), pp. 377–381. IEEE CS Press, Los Alamitos (August 2007)
14. Bondavalli, A., Ceccarelli, A., Falai, L.: Assuring Resilient Time Synchronization. In: Proc. of the IEEE Symposium on Reliable Distributed Systems (SRDS 2008), pp. 3–12. IEEE CS Press, Los Alamitos (October 2008)
15. Ficco, M., Coppolino, L., Romano, L.: A Weight-Based Symptom Correlation Approach to SQL Injection Attacks. In: Proc. of the 4th Latin-American Symposium on Dependable Computing (LADC 2009). IEEE CS Press, Los Alamitos (September 2009)
16. Scalp: Apache log analyzer, `http://code.google.com/p/apache-scalp/` (last update September 2009)
17. JMeter: Java application designed to load test web applications, `http://javaboutique.internet.com/tutorials/JMeter/`
18. Coral8 Engine,, at `http://www.aleri.com/sites/default/files/assets/product_literature/Coral8%20Engine.pdf` (last access October 2009)
19. Oracle CEP, `http://www.watersonline.com/public/showPage.html?page=800767` (last access December 2009)
20. The Borealis project, `http://www.cs.brown.edu/research/borealis/public/` (last access February 2010)

A Dynamic Key Agreement Mechanism for Mission Critical Mobile Ad Hoc Networking*

Ioannis G. Askoxylakis[1,2], Theo Tryfonas[2], John May[2], and Apostolos Traganitis[1]

[1] Foundation for Reserach and Technology-Hellas – Institute of Computer Science,
N. Plastira 100, 70013 Heraklion, Greece
`{asko,tragani}@ics.forth.gr`
[2] University of Bristol, Faculty of Engineering,
Queen's Building
University Walk,Clifton, Bristol, BS8 1TR
`{t.tryfonas,j.may}@bristol.ac.uk`

Abstract. Mobile ad hoc networks are expected to play an important role in demanding communications such as military and emergency response. In Mobile ad hoc networking each node relies on adjacent nodes in order to achieve and maintain connectivity and functionality. While offering many advantages, such as flexibility, easy of deployment and low cost, mobile ad hoc networking faces important security threats that could be proven vital in future telecommunication applications. This paper introduces a key dynamic agreement method based on a weak to strong authentication mechanism associated with a multi-party contributory key establishment method. It is designed for dynamic changing topologies, it employs elliptic curve cryptography to best serve thin clients with energy constrains, and reduces significantly key re-establishment due to network formation changes.

Keywords: MANET security, password authentication, elliptic curve cryptography, key agreement.

1 Introduction

Consider a disaster situation, such as an earthquake, a flood or a terrorist attack, where the commercial network infrastructure is destroyed or out of order and at the same time the need for establishing a network is crucial The objective of the rescue workers is to set up quickly, efficiently and easily a wireless network among themselves in order to help in a coordinated way the affected population. Their goal is to interconnect all their computing and communication devices, in a way that will enable them to share all necessary information securely, in a way that they could be sure that possible "high tech" terrorists/attackers in their range won't be able to disrupt or intercept the rescue efforts.

---

* This work was supported in part by the European Commission in the 7th Framework Programme through project EU-MESH (Enhanced, Ubiquitous, and Dependable Broadband Access using MESH Networks), ICT-215320, *http://www.eu-mesh.eu*

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 216–228, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

Security is a primary concern for providing protected communications to mobile nodes that operate in such hostile environments where there is no readily available infrastructure and where networks of varying sizes must be established quickly and dynamically. Moreover, there might be situations where potentially large numbers of rescue workers, potentially from multiple government services or even nations must cooperate and coordinate their efforts in areas where natural or man-originated disasters have damaged or set temporarily out of order part or the entire telecommunication infrastructure. The unique nature and characteristics of Mobile Ad-hoc Networks (MANETs) make them ideal networking solution to the above situations. At the same time their nature and characteristics pose a number of nontrivial challenges to their security design, architecture and services.

A MANET is a type of network, which is typically composed of equal mobile hosts that we call nodes. When the nodes are located within the same radio range, they can communicate directly with each other using wireless links. This direct communication is employed in a distributed manner without hierarchical control. The absence of hierarchical structure introduces several problems, such as configuration advertising, discovery, maintenance, as well as ad hoc addressing, self-routing and security [1].

In MANETs, such as in any other network trust cannot be provided among the nodes of the network without the existence of pre-defined prior known information to all nodes. This special kind of information is necessary in order to build trust between all participating nodes. A MANET is established among the existing nodes, if from preexisting, commonly known information, we reach a state where a common *session key* is agreed among the nodes.

The technical goal is to make sure that no other entity outside the *group* (*we define all the legitimate members of the established wireless network as group, e.g., soldiers of a military unit*) should be able to gain access within the new network. However, since neither a certification authority nor a secure communication channel exists, potential attackers have the ability to eavesdrop and modify exchanged messages transmitted over the air. Additionally, since no central identification authority is present, group member impersonation is easy, jeopardizing the security of the whole system.

Considering all these issues, the main challenge that arises is the setting up of a wireless network where the legitimate members of a group will be able to establish a protected wireless network. Moreover, in the case where a new node arrives at place, desiring to become a member in an already established group, joining, without delaying or even intercepting the existing group, is also challenging. The case where a group member is captured by the enemy and therefore the group key is compromised is also part of the considered scenario.

The rest of the paper is organized as follows: In section 2 we describe the adversary model and in section 3 we present the security requirements. In section 4, we present a review of the previous work concerning two-party and multiparty key agreements and we give a brief introduction on weak to strong authentication and the elliptic curve theory. In section 5 we describe the state of the art in multiparty key agreement protocols and particularly the d-cube and the aggressive d-cube algorithms and examine their properties and we describe our proposal that could be considered as an extension of both algorithms, designed for the dynamic changing topologies. Finally, in Section 6, we provide our concluding remarks along with suggestions for future work.

2 Adversary Model

As usual, the first step in the identification of security requirements is the understanding of the potential attacks against the network. This understanding is summed up in the following adversary model that describes the classes of attackers, their objectives, and their means to attack the system.

Attackers' classes. Taking into account the system model of a MANET we can identify tho types of attackers:

- External attackers: These are attackers that have no legitimate access to the MANET but they have appropriate equipment to use the wireless medium and interfere with the operation of the network protocols.
- Compromised nodes: These are legitimate node devices that have legitimate access to the MANET services and they have been compromised by attackers (e.g. by stealing a device or by capturing a legitimate user in the field) The attackers have the knowledge to modify the behavior of these nodes and try to take advantage of this in order to interfere with the operation of the network or to gain illegal access to its services

Objectives of attacks. We identify the following main objectives of attacks:

- Unauthorized access to the services provided by the MANET: Primarily, this objective is relevant for both classes of attackers.
- Unauthorized access to node data and meta-data: Here node data means the content of the messages exchanged in a service session, whereas meta-data refers to information on the nodes location and service usage profile (e.g., which applications are used and how often). Thus, the first objective is related to violating the confidentiality, and the second is related to violating the privacy of the node. Primarily, this objective is relevant for external adversaries.
- Denial-of-Service (DoS): This objective is related to degrading the QoS offered by the network (including the complete disruption of services). Primarily, this is relevant for external adversaries.

Attack mechanisms. There are a multitude of attack mechanisms that can be used and combined in order to reach the goals described above. However, most of these mechanisms fall into either one of the following two categories:

- Attacks on wireless communications (including eavesdropping, jamming, replay, and injection of messages, and traffic analysis);
- Compromising existing nodes (typically by physical tampering or logical break-in). The behavior of the fake or compromised nodes can be arbitrarily modified in order to help to achieve specific attack objectives .In such a scenario, the underlying security depends on the size and the randomness of the chosen password. However, the larger the password gets the more difficult it is to memorize and use. Moreover, since the response time is vital during emergency operations, the use of large passwords can be proved inconvenient. Therefore the use of short, user-friendly passwords is an essential requirement.

3 Security Requirements

It is broadly known that security mechanisms cannot create trust [2]. The members of a team that wish to establish a MANET know and trust one another physically. Otherwise, they would never be able to achieve mutual trust regardless of the authentication mechanism used. Our goal is to exploit the existing physical mutual trust in order to secure the ad hoc network.

A password authentication mechanism seems to be a rational approach that can deliver a proper solution without adding new requirements like the use of dedicated hardware (i.e smart cards). In a password based authentication scheme the use of a sufficiently large and randomly generated data string that can be used as a password would be an obvious approach. This way all nodes could agree on a password and, by using a trivial authentication protocol, achieve mutual authentication.

In such a scenario, the underlying security depends on the size and the randomness of the chosen password. However, the larger the password gets the more difficult it is to memorize and use. Moreover, since the response time is vital during emergency operations, the use of large passwords can be proved inconvenient. Therefore the use of short, user-friendly passwords is an essential requirement.

The use of short passwords provides weak authentication since the password selection set is quite limited and thus the corresponding authentication procedure is vulnerable to dictionary attacks [3]. Therefore, we need an authentication protocol that will lead to a reasonable degree of security even if the authentication procedure has been initiated from a small, weak password.

Below we outline the main security requirements of the proposed architecture:

Security architecture designed for thin clients. A MANET is typically composed of mobile devices with limited processing power and energy consumption. The cryptographic algorithms used for authentication and key agreement should have minimal impact in terms of computational overhead.

Weak-to-strong password-based authentication. Use of an authentication scheme that will lead to a reasonable degree of security although the authentication procedure has been initiated from a small, weak password.

Secure authentication. Only the entities that hold the correct password will eventually become members of the MANET.

Forward authentication. Even if a malicious partner manages to compromise a network entity in a later phase, he will still be unable to participate in the already existing network.

Contributory key establishment. The MANET is established when a session key is generated and agreed among all network nodes. The session key should be generated throughout in a contributory manner, by all participating entities.

Rare key re-establishment. Session Key refreshments should be performed as rare as possible, since during every new key re-establishment session the network is unavailable for node communications.

4 Related Work

4.1 Key Exchange and Elliptic Curve Cryptography

Common cryptographic protocols based on keys chosen by the users are weak to dictionary attacks. Bellowin and Merrit [4] proposed a protocol called *encrypted key exchange (EKE)* where a strong shared key is derived from a weak one. However, this protocol has a disadvantage. The creation of the common session key takes place with unilateral prospective, that is, only by the entity that first initiated the whole procedure. Thus the key agreement scheme is not contributory.

Diffie–Hellman is the first public key distribution protocol that opened new directions in cryptography [5]. In this important protocol for key distribution, two entities *A, B* after having agreed on a prime number p and a generator g of the multiplicative group Zp, can generate a secret session key.

An essential property for the majority of cryptographic applications is the need for fast and precise arithmetic. Calculations over the set of real numbers are slow and inaccurate due to round-off error [6]. Finite arithmetic groups, such as

$$F_p, F_{2^m}.$$

which have a finite number of points, is used in practice. All practical public-key systems today exploit the properties of arithmetic using large finite groups. Additionally, elliptic curves can provide versions of public-key methods that, in some cases, are faster and use smaller keys, while providing an equivalent level of security. Consequently, the use of ECC can result in faster computations, lower power consumption, as well as memory and bandwidth savings. This is very useful for mobile devices, like the ones used in ad hoc networks, which face limitation in terms of CPU, power, and network connectivity.

An elliptic curve [7] consists of elements (x, y) satisfying the equation:

$$y^2 = x^3 + \alpha x + \beta(\text{modp}). \tag{1}$$

for two numbers α, β. If (x, y) satisfies the above equation then $P = (x, y)$ is a point on the elliptic curve.

The elliptic curve discrete logarithm problem (ECDLP) can be stated as follows:

Fix a prime p and an elliptic curve E. Let xP represent the point P added to itself x times. Suppose Q is a multiple of P, so that $Q = xP$ for some x, then the ECDLP is to determine x given P and Q.

The general conclusion of leading cryptographers is that the ECDLP requires fully exponential time to solve. The security of ECC is dependent on the difficulty of solving the ECDLP.

Research community has given considerable attention to the ECDLP. Like the other types of cryptographic problems, no efficient algorithm is known to solve the ECDLP. The ECDLP seems to be particularly harder to solve. Moderate security can be achieved with the ECC using an elliptic curve defined over Z_p where the prime p is several times shorter than 230 decimal digits.

An elliptic curve cryptosystem implemented over a 160-bit field currently offers roughly the same resistance to attack, as would a 1024-bit RSA [8]. However, there have been weak classes of elliptic curves identified such as super singular elliptic curves [9] and some anomalous elliptic curves [10]. Implementations, such as ECDSA [11], merely check for weaknesses and eliminate any possibility of using these "weak" curves [12].

4.2 Elliptic Curve Diffie–Hellman

The original Diffie–Hellman (D-H) algorithm is based on the multiplicative group modulo p. However the elliptic curve Diffie–Hellman (ECDH) protocol is based on the additive elliptic curve group as desribed below. We assume that two entities A, B have selected the underlying field, $GF(p)$ or $GF(2^k)$, the elliptic curve *E* with parameters *a,b,* and the base point *P*. The order of the base point *P* is equal to *n*. Also, we ensure that the selected elliptic curve has a prime order to comply with the appropriate security standards [11].

At the end of the protocol, the communicating parties end up with the same value *K*, which represents a unique point on the curve. A part of this value can be used as a secret key to a secret-key encryption algorithm. We give a brief description of the protocol.

Entity *A* selects an integer,

$$d_A : d_A \in [2, n-2] \,. \tag{2}$$

Entity *B* selects an integer

$$d_B : d_B \in [2, n-2] \,. \tag{3}$$

A computes

$$Q_A = d_A \times P \,. \tag{4}$$

The pair Q_A, d_A consists A 's public and private key.

B computes

$$Q_B = d_B \times P \,. \tag{5}$$

The pair Q_B, d_B consists B 's public and private key.

A sends Q_A to B,

$$A : Q_A \rightarrow B \,. \tag{6}$$

B sends Q_B to A,

$$B : Q_B \rightarrow A \,. \tag{7}$$

A computes

$$K = d_A \times Q_B = d_A \times d_B \times P \,. \tag{8}$$

B computes

$$K = d_B \times Q_A = d_B \times d_A \times P\,. \tag{9}$$

Quantity K is now the commonly shared key between A and B. Moreover, it can also be used as a session key. Quantity n is the order of the base point P.

5 The Proposed Architecture

The dynamic topology of mobile ad-hoc networks introduces challenging security issues. The continuous flow of incoming and departing nodes is a key issue for designing a key agreement mechanism. Furthermore, when a node publicly claims that it is leaving the network it does not mean that it looses its ability to "hear" the messages exchanged among the remaining nodes, unless action is taken.

In all the approaches described in section 4, the only way to obtain a common session key when one or more modes depart from the established MANET, is to start over each algorithm from the very first step Furthermore, there are no intermediate session keys stored between nodes that are still part of the network, that could be proven to be useful for node-to-node communication, when global session key is no longer valid due to network reform. It is obvious that such approaches tend to be sufficient in relatively stable MANETs, where their topology does not change frequently. However, when network topology dynamicity increases, creating new global session keys very often would not be the best solution.

The proposed architecture proposes an efficient way for creation and use of intermediary session keys at the same time with the creation of the global MANET key, that can be used both for subgroup communications and as intermediate steps for key refreshment of the global session key, without the obligation to restart the group key agreement from scratch.

5.1 D-Cube Initiation

The proposed architecture is based on [16] and [17]. A session starts, based on either case, (d-cube algorithm or aggressive d-cube algorithm) and concludes with a common, contributory created, session key among all nodes of the MANET. It is best illustrated through a simple example which is depicted in figure 3.

Every node have a three bit address {x,x,x} a three bit mask, and is labeled from A to H. Its key contribution is represented by the corresponding lower-case letter.

Labels next to the arrows indicate the nodes that have already contributed, directly or indirectly, to the key. Suppose that player G (with address 110) is unsuitable (unavailable or does not know the password). In round 1, player H (111) will initiate the procedure of selecting as a partner the node whose address is 110 and mask 000.

The exchange attempt with G fails and the mask is already 000. So H does nothing in this round. In round 2, E (100) will start with (110) as candidate address and 001 as mask. The first recursive call will try 110 as candidate address and 000 as mask and will fail. The second recursive call will try 111 as candidate address and 000 as mask and will succeed. Similarly, in round 3 and figure 4, node C:010 starts partner finding with (110) as candidate. Asokan and Ginzboorg, in [16] also consider the case, where the total number of nodes is not more than 2^d, while the number of the faulty nodes is, $m: 2^k \leq m \leq 2^{k+1}$, for some $0 \leq k \leq d$. The 2^{k-1} of them are located in a single k-cube C_1 and the rest of them in a k-cube C_2.

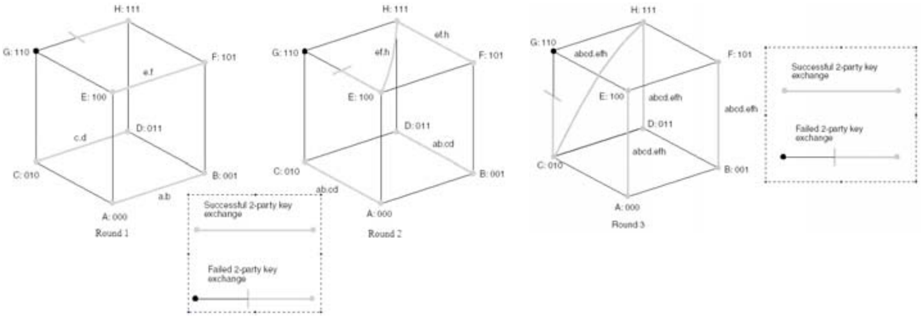


Fig. 1. 3-d cube rounds 1,2 and 3

The number of sub-rounds required in rounds from $k+2$ to d where $k < d-1$ are at most $m+1$ per round. This is because in each of those rounds, there is always one sub-round with m faulty partners. The same faulty node may select using N each of the m faulty partners in sequence before being able to complete its round exchange, thus resulting $m+1$ rounds. Since there is no other sub-cube with more faults, $m+1$ is the maximum number of sub rounds required.

In round $k+1$ the number of faulty players in C_1, is $2^k - 1$, resulting that the maximum number of sub rounds is 2^k. So the total number of sub-round for the first $k+1$ rounds is therefore

$$\sum_{j=0}^{k} 2^j = 2^{k+1} - 1. \tag{3}$$

Thus the total number of communication rounds required to complete the exchange is $2^{k+1} - 1 + (d-k-2)(m-1)$. This case incurs the maximum possible number of sub-rounds in the worst case during round 1 to $k+1$ round.

Next, we will detailed describe the aggressive 3-d cube example. (See fig.2) In this case we assume that node G is the faulty partner. During the first round the DH key exchange procedure performed between G:110 and H:111 will fail, since node G is a faulty one. However, instead of remaining idle and wait for the next round (as in the previous case), node H starts a DH key exchange with node E:100. Meanwhile Node E has already performed a successful DH key exchange with F:101, during the first half of the first round, so this key exchange will be the second successful one for this round. Node E having being notified by H that G is a faulty node will remain idle until the third round, instead of having attempted unnecessary DH exchanges with G.

In the next round (round 2) H performs a DH with node F and a DH with node C:010. Given that C has performed two successful DH with D:011 and H respectively, he will remain idle in the next round. However C has already performed a successful DH with A:000, during round one.

In total node C has performed three successful DH, with three different nodes, which means that C has completed all the appropriate procedures. Thus it will remain idle for the next round, which is the last round in our case. Summarizing the logic of this procedure we would say that the upper bound of the total successful DH procedures for a node participating in an aggressive d-cube algorithm is equal to d. In the described example d=3. During the third and final round there will be three more successfully accomplished DH key exchanges. One between H and D, one between F and B , and one between A and F.

Through this example it becomes obvious that using the aggressive 3-d cube algorithm, the faulty partner is being isolated. He only participates in one DH key exchange, the one performed in round 1 with node H, and since then he is excluded from all the subsequent DH key exchanges. Consequently, the faulty node loses the ability to have another change, during the generation process of the common session key, to compromise the security of the system.

In the following figures we give a graphical representation of the example.

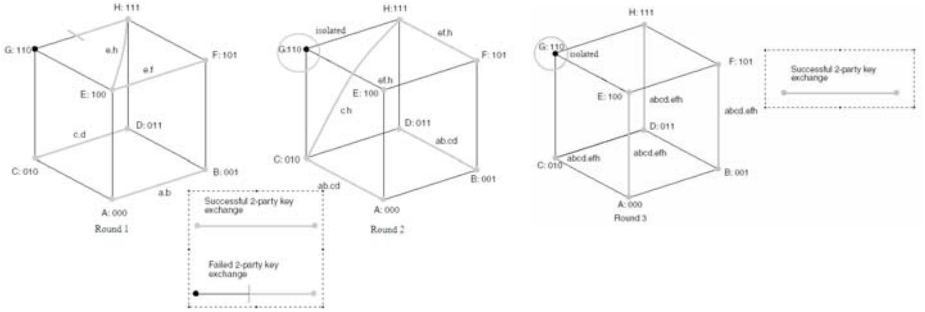


Fig. 2. Aggressive 3-d cube rounds 1, 2 and 3

5.2 Storage of All Intermediate Two-Party Keys

In the proposed algorithm, in contrast to [16] and [17] all intermediate two-party ECDH keys are stores by each node. This way, when a global session key has been created, every node in the d-dimensional cube maintains also a list of all the two-party ECDH keys that has created with every of her closest neighbors during the global key generation.

5.3 The Internal Tetrahedrons Integration

So far, as described in sections 5,1 and 5.2, as soon as the initial phase of the proposed algorithm is completed, each node posses the global session key, and the two party keys with her closest neighbors. At this point, if a node leaves the network, the global session key should be refreshed and in the meantime, secure communications are only available between couples of closest neighbors that participated in a two-party manner during the creation of the latest session key, which is no longer valid. This way, communication between distant neighbors, is only available through multi-hopping between nodes that in couples maintain valid two-party keys. This would add another requirement for routing metric information maintenance by all nodes, in order to serve each other to find the correct secure path in the network. Solution to this direction is provided by the proposed integration of tetrahedral group key agreement in the existing cubes. The proposed structure covers both cases (d-cube and aggressive d-cube) and takes place right after the creation of the global session key.

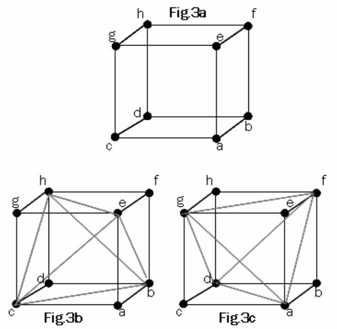


Fig. 3. The proposed tetrahedral algorithm structure

The procedure is the following:

As soon as the global session key has been created (round 3 in the 3-d example) all nodes establish two –party ECDH with their second level closer neighbors. There nodes are actually the ones based on the diagonal of each cubic surface. The algorithm is better demonstrated in figure 3. Figure 3a describes the cube created after the global key agreement, while figures 3b and 3c, demonstrate the two-party ECDH key exchanges, between the second order neighbors. All these additional two-party ECDH key exchanges form the two internal tetrahedrons inside the cube as shown in figures 3b and 3c. Figure 4, depicts the two internal tetrahedrons isolated by the cube. The process for the establishment of these tetrahedrons, in terms of two-party ECDH key agreements, is depicted in detail in figure 5. We can observe that two-party ECDH key agreements take place on non-connected segments. Although that after the second round the tetrahedrons have formed their global session keys, the algorithm has another final step, by covering all available segments.

This is due to two reasons: every node has a two party key with all nodes of the cube except the most distant node. For example, *a* has two party keys with every node of the cube except node *h*. Besides the group session keys among every 4 nodes forming a square edge of the cube, the four triangles of each internal tetrahedron shares a common session key, since the ECDH key exchange this time is thee party D-H key exchange instead of two-party in all other cases.

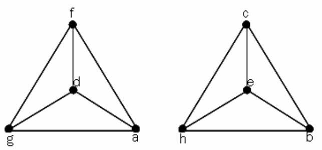


Fig. 4. The internal tetrahedrons

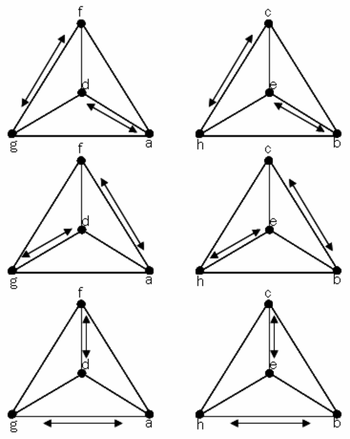


Fig. 5. The two-party ECDH key agreement sequence in the internal tetrahedrons

Let's provide an example to demonstrate the attributes of the proposed algorithm. The reference node for this example will be node *a*. During the initial 3-d or aggressive 3-d algorithm node a creates three two-party keys with nodes *b*, *c* and *e* and the global session key of the cube. During the tetrahedral algorithm node *a* creates three two-party keys with nodes d, g and f. This way node *a* maintains two-party keys with all nodes of the cube except h.

If any of its first and second order closest neighbor leaves the network, during the global key renewal node a will be still able to communicate with all expect one of the remaining nodes. However this distant node (in the example node *h*) belongs to the other tetrahedron and has keys for communication with the remaining nodes.

In another case if a decides to leave the network, her distant nodes, belonging to the left tetrahedron, do have keys for secure communications (a session key for the hole tetrahedron plus the two party keys among any pair of them), while the remaining three nodes *b*, *c* and *h* of the right tetrahedron, besides the two-party keys, they have a three-party key established among them during the last stage of the tetrahedral key agreement algorithm. Therefore, when a node leaves the network, the remaining nodes have all the two-party session keys, a four party session key of the tetrahedron that did not change formation, and a three party session key of the triangle composed of the three remaining nodes of the tetrahedron that the leaving node was part of.

6 Conclusion

Our research was motivated from the requirement of certain groups to establish fast, reliable, efficient and secure MANET's without relying on pre-existing infrastructures. The actual operational environment and the very nature of the established networks impose further key issues (e.g. the ability to add or subtract nodes depending on operational and security considerations) that need to be taken into account.

We have reviewed existing proposals around two-party or multiparty authentication and introduced a new key establishment method. Our proposal overcomes some of the main issues (such as rapid deployment, accuracy, and dynamic and robust behaviour) of existing solutions and operational environments. The proposed solution introduces the use of elliptic curve cryptography in such a scenario. ECC computations require less storage, less power, less memory, and less bandwidth than other systems. This allows implementation of cryptography in constrained platforms such as wireless devices, handheld computers, smart cards, and thin-clients. For a given security level, elliptic curve cryptography raises computational speed and this is important in ad hoc networks, where the majority of the clients have limited resources.

The proposed protocol meets all security requirements according the initial specification and it is stronger in terms of security. Finally, we have proposed secure and resilient architecture for dynamic MANETs, where the composition of the network changes in time with the arrival and departure of nodes. The secure dynamic recomposition of the network could become an important requirement in scenarios like battlefields where a soldier, under threat of capture, signs off the network on time.

The proposed tetrahedral algorithm can be applicable in several other scenarios such as for groups of people meeting in a room, (like students in a classroom, business meetings, mobile social networks etc). The password-based feature of our work could be used in cases where a group of people meets one another in person for the first time, and would like to go back home and set up a secure network among them.

The proposed algorithm leaves several open issues for future work. Formal analysis is necessary. The employment of the proposed internal algorithm to other algorithms like [18, 19] could also be useful. The incorporation of several new password-based key agreement protocols, which do not require the use of asymmetric encryption, is a challenging consideration. The dynamic case, where the network topology is rapidly changing, is also very interesting.

References

1. Verikoukis, C., Alonso, L., Giamalis, T.: Cross-Layer Optimization for Wireless Systems: A European Research Key Challenge. IEEE Communications Magazine 43(7), 1–3 (2005)
2. Bonnefoi, P.-F., Sauveron, D., Park, J.H.: MANETS: an exclusive choice between use and security? Special Issue on Interactive Multimedia & Intelligent Services in Mobile and Ubiquitous Computing (MUC) of Computing And Informatics 27(5) (2008)
3. Narayanan, A., Shmatikov, V.: Fast dictionary attacks on passwords using time-space trade-off. In: Proceedings of the 12th ACM conference on Computer and communications security, Alexandria, VA, USA (2005)

4. Bellovin, S.M., Merrit, M.: Encrypted key exchange: Password based protocols secure against dictionary attacks. In: Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, USA (May 1992)
5. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory 22, 644–654 (1976)
6. Cucker, F., Smale, S.: Complexity estimates depending on condition and round off error. Journal of the Association for Computing Machinery 46(1), 113–184 (2000)
7. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation 4(8), 203–209 (1987)
8. Rivest, R., Shamir, A., Adleman, L.M.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21(2), 120–126 (1978)
9. Menezes, A., Okamoto, T., Vanstone, S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory 39, 1639–1646 (1993)
10. Menezes, A., Teske, E., Weng, A.: Weak Fields for ECC. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 366–386. Springer, Heidelberg (2004)
11. Johnson, D., Vanstone, S.: The elliptic curve digital signature algorithm (ECDSA). International Journal on Information Security 1, 36–63 (2001)
12. Kalele, A., Sule, V.R.: Weak keys of pairing based Diffie-Hellman schemes on elliptic curves, Cryptology ePrint Archive 2005/30 (2005)
13. Zheng, D., Chen, K., You, J.: Multiparty authentication services and key agreement protocols with semi-trusted third party. Journal of Computer Science and Technology archive 17(6), 749–756 (2002)
14. Ateniese, G., Steiner, M., Tsudik, G.: New Multiparty Authentication Services and Key Agreement Protocols. IEEE Journal of Selected Areas in Communications 18(4) (April 2000)
15. Becker, C., Wille, U.: Communication complexity of group key distribution. In: 5th ACM Conference on Computer and Communications Security, San Francisco, California (November 1998)
16. Asokan, N., Ginzboorg, P.: Key agreement in ad hoc networks. Computer Communications 23, 1627–1637 (2000)
17. Askoxylakis, I.G., Kastanis, D.D., Traganitis, A.P.: Elliptic curve and password based dynamic key agreement in wireless ad-hoc networks, Communications, Networks and Information Security CNIS-2006, Cambridge, USA (October 2006)
18. Askoxylakis, I.G., Sauveron, D., Markantonakis, K., Tryfonas, T., Traganitis, A.: A Body-Centered Cubic Method for Key Agreement in Dynamic Mobile Ad Hoc Networks. In: Second International Conference on Emerging Security Information, Systems and Technologies, Cap Esterel, France, August 25-29, pp. 193–202 (2008)
19. Askoxylakis, I.G., Markantonakis, K., Tryfonas, T., May, J., Traganitis, A.: A Face Centered Cubic Key Agreement Mechanism for Mobile Ad Hoc Networks. In: First International ICST Conference on Mobile Lightweight Wireless Systems, MOBILIGHT 2009, Athens, Greece, May 18-20, pp. 103–113 (2009)

Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks

Giacomo de Meulenaer* and François-Xavier Standaert**

UCL Crypto Group
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium
{giacomo.demeulenaer,fstandae}@uclouvain.be

Abstract. Node capture is considered as one of the most critical issues in the security of wireless sensor networks. A popular approach to thwart the problem relies on the detection of events that arise during the attack such as the removal of a node for instance. However, certain attacks, such as side-channel attacks, might be furtive and defeat this type of defense. This work clarifies this question by performing a case study of power analysis attacks on AES and ECC implementations on two common types of nodes: the MICAz and the TelosB. From our experiments, the attacks can be carried out in a stealthy manner. As a result, stealthy node compromises should be considered when securing wireless sensor networks. Also, the moderate complexity of our attacks underlines the importance of low-cost side-channel countermeasures for sensor nodes.

Keywords: Wireless Sensor Networks, Node Compromise, Power Analysis Attacks.

1 Introduction

Wireless Sensor Networks (WSN) constitute a promising technology that enables the easy gathering and treatment of physical data from an environment. Integrated in wider networks, they offer the connectivity to the physical world in an easy and reliable way. They provide attractive solutions to many applications, including sensitive tasks such as perimeter protection, pollution detection, medical monitoring, etc. Within these networks, the sensor nodes are deployed in a potentially hostile environment and are therefore under the threat of various types of attacks. Among them, the node compromise is usually considered as one of the most challenging issues in the security of WSN [1].

In a node capture attack, an adversary tries to physically tamper with a node in order to extract the cryptographic secrets. This attack can be very harmful depending on the security architecture of the network. Moreover, it can give rise to many subsequent powerful insider attacks [2]. Two main directions exist to circumvent this important threat. The first one consists in improving the tamper

---

* Supported by Walloon Region project Nanotic.

** Associate researcher of the Belgian Fund for Scientific Research (FNRS-FRS).

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 229–242, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

resistance of the nodes in order to increase the effort of the attacker. However, tamper-resistant mechanisms are costly for small sensor nodes and are therefore usually not present on these devices. The second alternative adopts a surveillance-based approach, usually at the level of the network, which tries to detect events related to the node compromise. It assumes that a node capture will provoke some noticeable events, such as a loss of connectivity, a displacement or removal of a node, a loss of the node internal state, etc [2]. Defenses following this approach are attractive as they might even protect low-cost sensor devices vulnerable to physical attacks from the node capture attack. Such defenses are for instance proposed in [3,4] and [5,6], where a captured node is identified based on the detection of a suspicious behavior and a modification in its software code respectively. However, it remains to be verified whether any kind of node compromise really implies the detectable events upon which the defenses are built.

Side-channel attacks (SCA) may be able to avoid the detection of node compromise countermeasures. They are well-known to efficiently enable the recovery of the cryptographic secrets by exploiting the physical data available from the target device. In their passive form, these attacks are not supposed to interfere with the device operations. These attacks have been largely shown to be very efficient on a large variety of devices such as smart cards [7], PDAs [8], RFIDs [9], etc. So far, however, they have not been shown to enable stealthy node compromise in the context of WSN yet. As a result, the feasibility of these attacks in a furtive way remains to be assessed.

In this work, we clarify the question of possible furtive sensor node compromise by performing a case study of side-channel attacks in WSN. In particular, we carry out power analysis attacks on implementations of well-known cryptographic algorithms, the Advanced Encryption Standard (AES [10]) and the Elliptic Curve Cryptography (ECC [11]), on two popular sensor devices, the MICAz and the TelosB [12]. Using our setup, the attacks are not detectable by the usual surveillance-based node compromise defenses.

Organization. Section 2 first presents the related works and our contributions. Next, Section 3 explains the practical challenges of furtive SCA in WSN. Then, Section 4 explains our attack configuration to perform furtive SCA. Afterwards, Section 5 and Section 6 provide the results of our power analysis attacks on the MICAz and TelosB nodes. Section 7 later discusses the vulnerability of other nodes to these attacks. Finally, Section 8 analyzes the implications of stealthy node compromises on the security of WSN and Section 9 concludes this work.

2 Related Work and Contributions

The node capture attack has been illustrated in several works in the context of WSN. In [13], Hartung et al. recover the cryptographic secrets on a MICA2 sensor node by dumping its internal memory through the JTAG interface. The attack is extended in [14], where Becher et al. show how to access several node hardware components such as the external memory, the bootstrap loader or the

JTAG interface. They propose to disable the programming interfaces in order to prevent unauthorized accesses to the microcontroller. They underline that the node capture requires the absence of the node from the network for a substantial period, which could be useful to detect captured nodes.

In [15], Goodspeed relates that some sensor node transceivers embedding a cryptoprocessor present major weaknesses. The secret key can be extracted by sniffing the SPI bus between the transceiver and the microprocessor or by gaining access to the transceiver internal memory through the debugging interface.

Software-based attacks can also efficiently compromise nodes. In [16], Gu and Noorani introduce an attack by means of *mal-packets*, which exploit a buffer overflow to remotely perform a limited and transient execution of an external code. This attack is extended in [17], where Francillon et al. describe a powerful remote code injection attack that permanently injects an arbitrary malicious code on the targeted sensor.

All the node capture attacks mentioned above (except the bus sniffing attack) have the particularity of provoking a noticeable event during the attack, such as a temporary exclusion of a node from the network or a modification in the memory of a sensor device. Therefore, a class of countermeasures has emerged, based on the assumption of detectable node captures. Several countermeasures against node capture are based on this observation, such as the defenses proposed in [14,4].

Side-channel attacks have drawn relatively little attention in the context of Wireless Sensor Networks. In [18], Okeya and Iwata point out the importance of side-channel attacks for sensor devices and show how message authentication codes can be attacked with power analysis in a chosen-plaintext attack scenario. More general side-channel attacks on sensor nodes are listed in a taxonomy by Pongaliur et al. in [19] but their potential to enable stealthy attacks has not been demonstrated in a practical study yet.

Contributions. Following these works, the contributions of this paper are:

1. We practically prove the feasibility of stealthy node compromises in the context of WSN. We analyze the implications of these attacks and discuss the main directions that can be followed to secure WSN against them.
2. We illustrate the efficiency of side-channel attacks within the framework of WSN. Our case study clarifies the effort required by the attacker to capture a node with power analysis attacks. The moderate complexity of our furtive attacks underlines the need of robust and low-cost protections against side-channel attacks for sensor nodes.

3 Stealthy Side-Channel Attacks

Side-Channel Attacks (SCA) are well-known to be efficient against unprotected cryptographic implementations. Advanced SCA are now able to break many cryptographic primitives with a small number of physical data records (or traces).

For instance, the most advanced power analysis attacks performed in [20] break unprotected implementations of the symmetric block cipher AES on 8-bit microcontrollers with less than 10 traces. Unprotected implementations of public key cryptography, such as Elliptic Curve Cryptography (ECC) [11], may even face a key recovery based on a single trace using Simple Power Analysis [21].

Side-channel Attacks are usually carried out in a context where the attacker can control the target device, at least briefly. This is not possible in the context of stealthy attacks in WSN. Indeed, to remain furtive, the attacks must be performed on-site and without generating any of the detectable events listed earlier. The specificities of the WSN scenario can be challenging for an adversary for the following reasons:

- **Passive acquisition:** Achieving fully passive SCA might be difficult with the usual measurement setups. For instance, power analysis classically requires the insertion of a small resistor in the power line, depackaging the chip might be needed to efficiently measure electro-magnetic emanations, etc. This should be done without disrupting the device operations.
- **On-site acquisition:** The target node cannot be moved to a convenient place to carry out the attack (typically, in a laboratory). Instead, the attacker must bring his equipment to the target node, the accessibility of which depends on the context. Moreover, his presence at the target node might reveal the attack.
- **Device not controlled:** The attack should be feasible based on known ciphertexts and a few measurements since the frequency of use of the cryptographic primitive is beyond the control of the adversary. Moreover, the extraction of the useful portions in the acquired physical data cannot be made easier by the use of adversary controlled triggers.
- **Real-world device:** With respect to a board dedicated to side-channel analysis, more noise is expected due to the presence of many components working simultaneously. Also, elements filtering the power supply make power analysis more difficult.

In the following, we describe how these challenges can be surmounted with our case study of furtive power analysis attacks.

4 Attack Configuration

Before focusing on the scenario and the setup of our stealthy power analysis attacks, we briefly describe the sensor node platforms used in this work.

4.1 Sensor Node Platforms

Sensor nodes are mainly composed of a microcontroller, a transceiver, a battery, an external memory and sensors. As the currently available platforms embed various types of hardware, we chose two representative sensor node platforms: the MICAz and the TelosB [12]. Interestingly, their microprocessors have different

Table 1. Features of the MICAz and TelosB sensor nodes

Device	Microcontroller (Freq. , RAM)	Transceiver (Throughput)	Software
MICAz [12]	ATmega128L (7.37MHz, 4kB)	CC2420 (250kbps)	TinyOS
TelosB [12]	MSP430 (4MHz, 10kB)	CC2420 (250kbps)	TinyOS

word sizes : 8-bit for the MICAz and 16-bit for the TelosB. Both nodes support the popular TinyOS operating system and share the same CC2420 transceiver. Their main design features are displayed in Table 1.

4.2 Attack Scenario

We consider a typical WSN scenario where the nodes periodically send a report concerning the acquired data. The packets are encrypted with AES and ECC is used to establish shared secret keys between pairs of nodes. For simplicity, we restrict ourselves to the case where the on-site acquisition is convenient for the adversary: the nodes are easily accessible and the presence of the adversary at the target node is not detected (e.g., in a large outdoor WSN).

4.3 Attack Setup

For the acquisition of the power traces, we replaced the node power supply with a supply containing a 10-Ω sense resistor in its circuit. To obtain meaningful traces, we had to remove several capacitors and inductors filtering the power supply. Special care was taken to prevent any transient failure in the power supply while handling its circuit. In this view, we temporarily introduced an additional power supply line to go on feeding the node components while interrupting the original power line. This temporary supply line is shown in Figure 2 for the TelosB. To avoid the introduction of a short circuit while unsoldering, an independent power supply was used for the soldering iron.

Throughout these manipulations, we checked the stability of the supply voltage with an oscilloscope. Only minor variations were observed. The smooth running of the node was also verified by checking the regularity and the content of the broadcasted messages. As a result, the introduction of our measurement setup does not provoke any significant event: it therefore defeats the proposed surveillance-based node capture defenses.

Remark that it appears feasible for an attacker to put the node board back in its original state in order to avoid any subsequent visual detection of the attack.

Our measurement setup is shown in Figure 1. The voltage drop across the resistor is measured on a Tektronix TDS7104 oscilloscope at a sampling frequency of 250 MHz. A more portable device could be used, like a PC-based oscilloscope for instance [22].

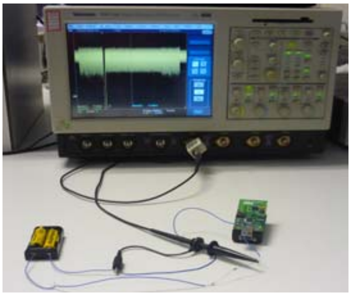


Fig. 1. Measurement setup of our power analysis attack on the TelosB node

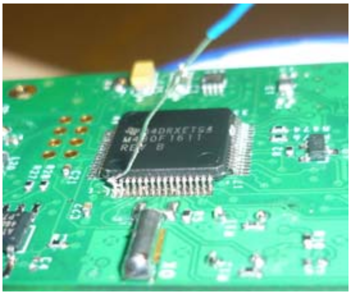


Fig. 2. Detail of the TelosB with its temporary supply line introduced to go on feeding the node while interrupting its original supply circuit

5 DPA Attack on AES

Our first attack concerned a Differential Power Analysis (DPA [21]) on a software implementation of AES on the MICAz and TelosB. We first shortly describe the DPA attack, then explain how it was achieved based on the attack configuration of Section 4 and finally present the results and the applicability of the attack.

5.1 Description

The DPA attack is the most popular power analysis attack. Its inputs are a sufficient number of traces of the cipher and the corresponding plaintexts (or ciphertexts). This attack exploits the data dependency of the power consumption. It targets a cipher round key, which is attacked by pieces, called subkeys (typically the key bytes). For each of the plaintexts (or ciphertexts), predictions of the power consumption are stated for every possible subkey. These hypothetical consumptions are then compared with the acquired traces with a statistical test, such as the correlation coefficient, which measures the linear relationship between two random variables [23]. The closest hypothetical consumption leads to the right subkey guess if there are sufficient traces. The recovery of the full round key easily reveals the AES main key. A detailed description of the DPA attack can be found in Chapter 6 of [21].

5.2 Implementation in the Context of WSN

The DPA attack performed in this work was based on the ciphertexts broadcasted by the target node and the traces acquired using the setup described in Section 4. The collection of the ciphertexts allowed the attack on the last round key. Inverting the AES key schedule led to the main key.

The rough trigger used to acquire the power traces was the brief transmission state of the node transceiver. However, a DPA requires well aligned traces such that the time samples of all traces correspond to the same instructions.

Resynchronizing the traces was successfully performed using a pattern matching method suggested in Section 8.2.2 of [21]. This method finds the correct relative position of a trace with respect to another one by minimizing their mean square error. This technique appeared to be very precise.

5.3 Results

Our own implementation of AES with 128-bit keys was the target of our DPA attack. It is written in TinyOS and is reasonably efficient. It requires a moderate memory occupation (272 B of RAM and about 1kB of ROM on both devices).

The attack was shown to succeed with a relatively small complexity in terms of required power traces. We illustrate its results for the first subkey in Figures 3 and 4 on the MICAz and TelosB respectively. In these figures, the correlation coefficients of each of the 256 subkey guesses are plotted in function of the number of traces on the point of interest in the traces which provides the larger correlation for the correct subkey guess. The coefficient of the right guess remains at a high value (around 0.7) while the coefficients of the wrong guesses converge to lower values. It is already clearly distinguishable with less than 20 traces for the MICAz and 60 traces for the TelosB. Deducing the number of required traces for a successful attack from these figures is not adequate if the attacker does not know the point of interest in the traces. Therefore, we also studied the complexity of the attack when this point is unknown beforehand. In this case, all subkeys were recovered with about 40 traces and 80 traces on the MICAz and TelosB respectively.

The higher complexity for the TelosB was expected, considering its 5-fold inferior power consumption [24]. Moreover, its 16-bit word size is superior to the number of bits considered in a subkey (i.e., 8). Therefore, the 8 remaining bits cause a power consumption that is not considered in the power model, usually denoted as algorithmic noise. This noise is not present on the MICAz because of

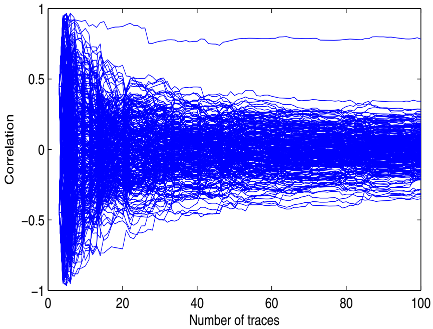


Fig. 3. Correlation coefficients of the 256 subkey guesses in function of the number of traces (MICAz). The right guess is already visible with less than 20 traces.

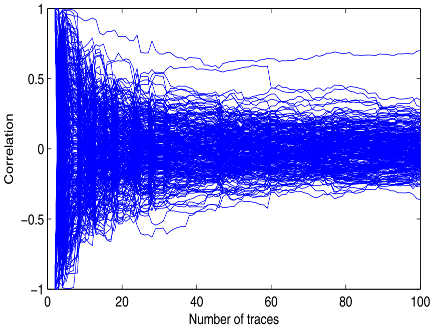


Fig. 4. Correlation coefficients of the 256 subkey guesses in function of the number of traces (TelosB). The right guess is already visible after 60 traces.

its 8-bit word size microcontroller. The small complexity of our DPA attack on sensor devices is in fact of the same order of magnitude as these obtained in [20] for advanced DPA attacks on small 8-bit microcontrollers.

5.4 Applicability in a Practical WSN Scenario

Our DPA attack against AES on the MICAz and TelosB has a complexity in terms of traces that is clearly within the reach of an attacker. Even for nodes transmitting encrypted messages infrequently, acquiring the sufficient number of traces appears to be realistic. For instance, in an application where nodes transmit a packet every 10 minutes, the secret key of a TelosB can be recovered by an attacker in about $80 \cdot 10/60 \approx 13$ hours with our DPA attack. Conversely, a MICAz transmitting a packet every second is exposed to a key recovery within a few minutes.

6 Template-Based SPA Attack on ECC

Our second attack was a template-based SPA attack on ECC [25]. We first explain the attack, then detail how we implemented it in the context of WSN. After that, we expose the attack results on the MICAz and TelosB and the relevance of the attack in a practical WSN context.

6.1 Description

The point multiplication is the basic operation of ECC. It is usually computed by iterations, in which an intermediary point can be transformed in several possible points, depending on one or few key bits (see [11]). It can be attacked in one trace with the Simple Power Analysis. This technique exploits the dependency on operations of the power consumption. However, most implementations of ECC include optimizations, such as windowing (see Section 3.3 in [11]), which prevent the recovery of the full key using SPA.

The template-based SPA, which relies on the dependency on both operations and data of the power consumption, can be a powerful alternative to SPA to obtain the full key in one trace, as suggested in Section 4.3 of [25]. It begins with the online phase of the attack, i.e., the acquisition of a single ECC trace on the target device. Then the offline phase of the attack is performed, made of the following two steps, repeated for each iteration of the point multiplication (starting with the first iteration):

- **The template building step.** First, the attacker builds templates corresponding to the computation of an iteration of the point multiplication. Templates are statistical models deduced from traces for a subset of the key space. They are collected offline on a similar device running the same implementation (see Section 5.3 in [21] for more details).

- **The template matching step.** After that, the templates are compared with the trace acquired in the online phase. As templates correspond to the computation of the possible iteration results, this comparison determines which intermediary values were actually computed by the target device, leading to the recovery of the key bits involved in the iteration.

To achieve these steps on an iteration, the iteration input point has to be known. This is not a problem for the first iteration since its input point is a known parameter. For the other iterations, the intermediary point is revealed by the matching step of the previous iteration. When all the iterations are successfully processed, the full key is obtained.

6.2 Implementation in the Context of WSN

The online phase of the attack was carried out using our setup of Section 4. As ECC operations are infrequent, we relied on the format of the exchanged messages to roughly select the portion of the power consumption corresponding to ECC calculations.

Concerning the offline phase, the templates were built from the acquisition of traces on a similar node running the same implementation (the TinyECC library [26]). To achieve the matching step, a precise synchronization is required between the templates and the corresponding portion of the trace. In this view, we used the same technique as in the case of the DPA: The correct template is assumed to match the corresponding portion of the trace and thus minimize their mean square error when their correct relative position is found. Our experiments proved that this method was accurate, as depicted in Figure 5 for the TelosB.

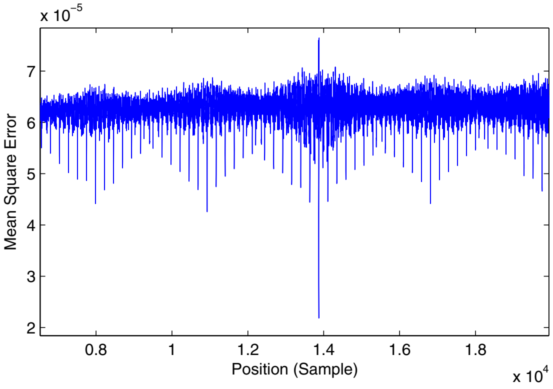


Fig. 5. Mean Square Error between the correct template and the reference power trace when synchronizing them (TelosB). The lowest error clearly reveals the right relative position.

6.3 Results

In our experiments, we carried out the online phase of the attack and the offline phase for the first iteration of the point multiplication. As the same attack steps are repeated for all the iterations, focusing on one iteration is enough to determine the feasibility of the whole attack.

In the building step, we built two templates as one single key bit was handled per iteration of the point multiplication under attack. For this, we collected on a similar device a set of 100 traces for each of the two possible results. Then, in each of these sets, we selected the sequences of samples corresponding to the targeted iteration and averaged them. To speed up this process, we restricted the template size to 100,000 samples.

In the template matching step, we compared our two templates with the trace obtained in the online phase. The criterion used to determine which intermediate point was actually computed in the iteration was the least-square test between the trace samples of interest and the two templates. As indicated in [21], this test can be seen as a maximum-likelihood decision rule.

The matching step successfully led to the recovery of one key bit on the MICAz and TelosB. Repeating the matching step 100 times showed that the targeted key bit could be recovered with very high confidence. Consequently, the whole attack appears feasible on both platforms.

6.4 Applicability in a Practical WSN Scenario

The online complexity of the attack is minimal. With the measurement setup described above, an attacker only needs to wait for a single ECC operation on the target node.

In the offline phase, the adversary does not face the detection of the attack any more. This phase requires the access to a identical device running the same ECC implementation. It is realistic assuming commercially available nodes (or at least, their microcontrollers) and the use of a freely available ECC implementation, such as the TinyECC library [26] that we used in this work. With 160-bit keys, our choice of 100 traces per template leads to $100 \cdot 2 \cdot 160 = 32000$ traces to acquire on the similar device. This can be done within $32000/3600 \approx 9$ hours with an automated setup acquiring one trace per second. The complexity of the offline phase is thus perfectly reachable for an attacker. As a result, the template-based SPA can be a severe threat to ECC implementations in the context of WSN.

7 Other Nodes

The current generation of sensor nodes is constituted by many heterogeneous devices. Apart from the platforms based on 8-bit or 16-bit microcontrollers as the MICAz and TelosB studied in this work, other larger nodes exist, that are based on 32-bit more powerful microcontrollers, such as the Sun SPOT [27] or the IMote 2 [12]. These platforms differ from usual smaller nodes by being much less restricted in terms of computation and memory constraints. For instance, the ARM 920T of the Sun SPOT runs at 180MHz and contains 512kB of RAM.

These devices, based on the standard CMOS technology, do not have inherent protection against side-channel attacks. In the literature, many attacks have been successfully applied on 32-bit based embedded device. For instance, the template-based SPA of Medwed et al. [25] is carried out on a 32-bit ARM7 processor. Therefore, the vulnerability of these larger nodes to furtive side-channel attacks is real. However, the larger word size of their processor should make the attacks more difficult, because of a larger algorithmic noise. The more powerful nodes are also better equipped to resist to side-channel attacks because of their larger memory resources, which could include advanced (and costly) countermeasures.

8 Implications

The feasibility of stealthy node compromises has major implications on the security of WSN. By nature, these attacks cannot be thwarted by the existing surveillance-based node capture defenses. These countermeasures are however far from being useless as they prevent many kinds of node compromise. Moreover, they also prevent an adversary from actively speeding up the acquisition phase of furtive SCA (e.g., by injecting messages to stimulate the use of the cryptographic primitives on the target node).

Stealthy node captures enable an adversary to compromise node-by-node large parts of unprotected networks. WSN should thus be protected against these severe attacks. For this purpose, we identify three approaches.

1. Side-channel countermeasures could be added on the nodes to complicate the recovery of the secret keys. They are usually not included in cryptographic implementations for sensor nodes (with the notable exception of [28]). These defenses should have a moderate cost and be hopefully as strong as the cryptographic algorithms employed. Their level of security should be known and properly assessed.
2. A second possibility would be to use security protocols tolerant to node capture attacks. This approach is not new. For instance, the protocol presented in [29] considers an adversary model where an attacker is able to compromise a limited number of nodes, without making any assumption regarding the node capture process. However, such protocols may be hard to achieve depending on the functionality of the protocol.
3. Finally, the conditions of stealthiness of the attack could be repressed. One could assure that the nodes are never left without visual surveillance, but it may be costly depending on the application and the size of the network. Onboard defenses could be provided to attempt to detect when the nodes are being attacked. While not capable of totally preventing stealthy attacks (at least, electro-magnetic emanations could still be exploited in an attack [30]), these defenses could significantly increase the effort for the attacker. However, their cost may be significant.

Protecting WSN against stealthy node compromises seems thus a non-trivial problem. A combination of defenses at the level of the network and in the nodes themselves is likely to offer the highest level of security in WSN.

9 Conclusion

In this work, we prove the feasibility of furtive power analysis attacks in the context of WSN. Using our setup, these attacks can be undetectable for surveillance-based node capture defenses. While limited to situations where the nodes are easily accessible and the adversary presence is not detected, they remain of concern in many realistic scenarios of WSN. They involve the manipulation of the power supply circuit without disturbing the node, which can be challenging if some of its components are hard to access. However, for a skilled adversary, the furtive power analysis attacks represent a really attractive option: the amount of power traces to record is small, as illustrated in our attacks on AES and ECC implementations on the MICAz and TelosB.

The existence of furtive physical attacks seriously jeopardizes the security of WSN. To remain secure, WSN should either use security protocols which tolerate stealthy node compromises or make use of nodes that are protected against these attacks. Our work underlines the need of robust and low-cost side-channel defenses for small devices like sensor nodes.

Acknowledgments. The authors thank Johann Groszschädl and Nicolas Veyrat-Charvillon for their helpful comments and suggestions.

References

1. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. ACM Commun 47(6), 53–57 (2004)
2. Krauß, C., Schneider, M., Eckert, C.: On handling insider attacks in wireless sensor networks. Inf. Secur. Tech. Rep. 13(3), 165–172 (2008)
3. Khalil, I., Bagchi, S., Nina-Rotaru, C.: DICAS: Detection, Diagnosis and Isolation of Control Attacks in Sensor Networks. In: 1st Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks, SECURECOMM (2005)
4. Conti, M., Pietro, R.D., Mancini, L.V., Mei, A.: Emergent properties: detection of the node-capture attack in mobile wireless sensor networks. In: WiSec 2008: 1st conference on Wireless network security, pp. 214–219. ACM, New York (2008)
5. Seshadri, A., Perrig, A., Van Doorn, L., Khosla, P.: Swatt: Software-based attestation for embedded devices. In: Proceedings of the IEEE Symposium on Security and Privacy (2004)
6. Krauß, C., Stumpf, F., Eckert, C.M.: Detecting node compromise in hybrid WSN using attestation techniques. In: Stajano, F., Meadows, C., Capkun, S., Moore, T. (eds.) ESAS 2007. LNCS, vol. 4572, pp. 203–217. Springer, Heidelberg (2007)
7. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers 51(5), 541–552 (2002)

8. Gebotys, C.H., Ho, S., Tiu, C.C.: EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 250–264. Springer, Heidelberg (2005)
9. Hutter, M., Mangard, S., Feldhofer, M.: Power and EM attacks on passive 13.56 MHz RFID devices. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 320–333. Springer, Heidelberg (2007)
10. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, Heidelberg (2002)
11. Hankerson, D., Menezes, A.J., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer, New York (2003)
12. CrossBow. Wireless Sensor Networks Module Portfolio, `http://www.xbow.com/Products/productdetails.aspx?sid=156`
13. Hartung, C., Balasalle, J., Han, R.: Node compromise in WSN: The need for secure systems. Technical Report CU-CS-990-05, Colorado University (2005)
14. Becher, E., Benenson, Z., Dornseif, M.: Tampering with motes: Real-world physical attacks on wireless sensor networks. In: Clark, J.A., Paige, R.F., Polack, F.A.C., Brooke, P.J. (eds.) SPC 2006. LNCS, vol. 3934, pp. 104–118. Springer, Heidelberg (2006)
15. Goodspeed, T.: Extracting keys from second generation zigbee chips. Work in progress, Black Hat USA (2009), `http://www.blackhat.com/presentations/bh-usa-09/GOODSPEED/BHUSA09-Goodspeed-ZigbeeChips-PAPER.pdf`
16. Gu, Q., Noorani, R.: Towards self-propagate mal-packets in sensor networks. In: WiSec 2008: Proceedings of the first ACM conference on Wireless network security, pp. 172–182. ACM, New York (2008)
17. Francillon, A., Castelluccia, C.: Code injection attacks on harvard-architecture devices. In: CCS 2008: Proceedings of the 15th ACM conference on Computer and communications security, pp. 15–26. ACM, New York (2008)
18. Okeya, K., Iwata, T.: Side channel attacks on message authentication codes. In: Molva, R., Tsudik, G., Westhoff, D. (eds.) ESAS 2005. LNCS, vol. 3813, pp. 205–217. Springer, Heidelberg (2005)
19. Pongaliur, K., Abraham, Z., Liu, A.X., Xiao, L., Kempel, L.: Securing sensor nodes against side channel attacks. In: HASE: Proceedings of the 11th IEEE High Assurance Systems Engineering Symposium, pp. 353–361 (2008)
20. Standaert, F.-X., Gierlichs, B., Verbauwhede, I.: Partition vs. Comparison Side-Channel Distinguishers:an Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 253–267. Springer, Heidelberg (2009)
21. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer, New York (2007)
22. PicoTechnology. Portable High Perf. PC Oscilloscope (January 2010), `http://www.picotech.com/picoscope5000.html`
23. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
24. de Meulenaer, G., Gosset, F., Standaert, F.-X., Pereira, O.: On the energy cost of communication and cryptography in wireless sensor networks. In: WIMOB 2008: Proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, Washington, DC, USA, pp. 580–585. IEEE Computer Society, Los Alamitos (2008)

25. Medwed, M., Oswald, E.: Template attacks on ECDSA. In: Chung, K.-I., Sohn, K., Yung, M. (eds.) WISA 2008. LNCS, vol. 5379, pp. 14–27. Springer, Heidelberg (2009)
26. Liu, A., Ning, P.: TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In: IPSN, pp. 245–256 (April 2008)
27. SUN. Sun SPOT (Sun Small Programmable Object Technology) (September 2009), `http://www.sunspotworld.com/`
28. Lederer, C., Mader, R., Koschuch, M., Großschdl, J., Szekely, A., Tillich, S.: Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks. In: Markowitch, O., Bilas, A., Hoepman, J.-H., Mitchell, C.J., Quisquater, J.-J. (eds.) Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks. LNCS, vol. 5746, pp. 112–127. Springer, Heidelberg (2009)
29. Parno, B., Perrig, A., Gligor, V.: Distributed detection of node replication attacks in sensor networks. In: SP 2005: Proceedings of the 2005 IEEE Symposium on Security and Privacy, Washington, DC, USA, pp. 49–63 (2005)
30. Quisquater, J.-J., Samyde, D.: ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In: Attali, S., Jensen, T. (eds.) E-smart 2001. LNCS, vol. 2140, pp. 200–210. Springer, Heidelberg (2001)

Sensor Networks – Critical Infrastructure for Society? Challenges for Resilience, Security and Interoperability

Alistair Munro

EADS DS (UK) Ltd., The Quadrant, Celtic Springs Business Park, Coedkernew, Newport,
South Wales, UK, NP10 8FZ
`alistair.munro@eads.com`

Abstract. Sensor networks have evolved rapidly in recent years from purpose built technology specific deployments to the stage where they are now able to deliver information through commodity communications channels. In parallel, pressures on the environment and resources have made the range of such purposes much wider and sensor input is necessary for sustainability of society's functions and infrastructure. The sensor network is becoming a part of critical network infrastructure and, in the same ways as other supporting technologies, must satisfy requirements for resilience, security and interoperability. This paper takes stock of requirements and solutions to highlight the opportunities and potential threats that follow from these trends. It reports on current work in CENELEC on a framework for addressing these issues.

Keywords: Sensor networks, resilience, security, interoperability.

1 Introduction

Sensor networks are widely installed in the world in urban, suburban and rural locations on the ground and in various airborne platforms, including balloons, high-altitude platforms (HAPs), unmanned airborne vehicles (UAVs) and satellites.

At present few of them have a purpose that involves real-time interaction with human beings. The Internet of Things will change this and make sensors, and actuators, first class devices, fully visible with end-to-end connectivity. We will depend on their capabilities and the data they provide for healthcare, energy management, environmental monitoring, transportation, homeland security and many other aspects of life.

Our assumption accordingly is that they are inevitably becoming a part of critical infrastructure. The motivation therefore for this paper is to explore the nature of, and challenges to, the processes that measure and control this dependency. The resilience of these systems will become a key discriminator of their quality and performance in achieving a positive or negative view of our reliance on them.

It is thus necessary to make sure that the sensor network applications operating over critical infrastructure are protected effectively as well as being thoroughly tested and correctly planned and deployed. If this is achieved then we can expect:

- Resilience of society's key functions:
- Improved situational awareness in anticipating and reacting to imminent events;

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 243–253, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

- Better understanding of strengths, weaknesses, new opportunities, threats;
- Much more information available, so decision support is improved and reactions are higher quality;
- Systems are more efficient and cost-effective.

If it is not achieved then we risk:

- Dependency on systems that are not fit for purpose;
- Reduced security: less critical for disconnected systems, but essential when interconnected;
- Many kinds of attack: intrusion, denial of service, interception, masquerading;
- Poor interoperability – devices do not work together;
- Service level agreements not clear – the communications support may be inadequate or, at the other extreme, over-specified;
- Loss of privacy and confidentiality.

We begin with an overview of sensor networks in order to articulate the key issues in Section 2. The following sections focus on two key topics: Section 3 looks at vulnerabilities of the sensor communications system, and Section 4 discusses interoperability issues. Section 5 presents conclusions and topics for future study.

2 Sensor Networks – A Big Topic

As Akyildiz et al. have observed [1], significant opportunities have been created for systems composed of small, untethered sensor nodes, communicating over short distances using wireless media, by advances in micro-electro-mechanical transducers and actuators, wireless communications, and processing power of embedded digital electronic information processing devices. These are collectively termed wireless sensor networks (WSN).

Interesting problems arising from these opportunities have motivated extensive research into the communications aspects of WSN, of which resilience and performance is an important part, especially in terms of routing, data fusion and security. However WSN are not completely representative of a collection of technologies that is already well established and very widely deployed. Furthermore, the acquisitions of data is just the starting point for feeding it into the collection of applications that will use it. We will come to depend on these systems and the services they provide as part of society's critical infrastructure. Some illustrations of such systems and their vulnerabilities are given below:

- Electronic commerce: buying and selling, the banks and the financial sector. These are some of the biggest users of secure networked communications and they suffer persistent and sophisticated attack. Future e-commerce, online and on the move, will involve interaction of the financial systems with products and users to exchange identities, keys, and information about price, credit, user-guides and so on. Products will be equipped with RFID capability to store this information; and mobile personal devices will sense this information, exchange keys with local point-of-sale terminals, which will themselves interact securely on an open medium with the back-office enterprise system, e.g using UMTS.;

- The police, immigration, homeland security and other security services, the emergency services. This sector increasingly uses information from sensors, e.g. streaming CCTV, and other distributed services with an autonomous distributed machine-to-machine (M2M) component to gather intelligence from the environment. They require priority access to communications services, often needing to displace ordinary users and applications;
- Transportation, including highways, inshore water, railways, and civil aviation. The networking of transportation services is well established in certain infrastructure areas: toll collection by radio tag, traffic monitoring, signalling. Communication with, and between, road vehicles, boats and trains, including trams, is taking shape. There are requirements that are similar to those for civil aviation, e.g. collision avoidance. Wireless communications standardisation is quite advanced at the lower layers, e.g. CALM for road vehicles, or GSM-R for railways. Networking is largely focussed on IPv6;
- Resources, such as electricity, gas, oil, water and heat. The industry and governments are struggling to find a solution that will allow resources to be managed proactively, first for meter interoperability, the home sensor/actuator appliance network, and second for the communications network. There are interest groups, such as SmartGrids, supported by the EU Commission, and ongoing work in CENELEC in the Smart Meter Coordination Group;
- Environment, including: quality of air and water; disaster anticipation, first-response and recovery (fire, flood, earthquake, storm, attack – US Department of Homeland Security lists about 20 categories as well as civilian events). For monitoring, sensor networks are already deployed widely: wired and wireless terrestrial for a range of physical quantities on the ground; low to high altitude platforms, e.g. balloons, UAVs, for the lower atmosphere and short-range EO/IR, LIDAR and multi-mode sensing of ground state; and satellites for remote sensing;
- Health, including the enterprise, (public and commercial), telecare, and e-health. Experts from the healthcare institutions and from national and local government stress the demographic deficit that is heading our way: there will not be enough able-bodied people to take care of an aging population. Security is a particularly sensitive area: information harvested from sensors that was formerly private between a patient and a doctor now circulates on networks of various kinds.

While each of these sensor network applications has its own problems with security and vulnerabilities to attack, in general the resilience challenges focus on a two priority topics:

- Vulnerabilities affecting security and resilience at different layers of the communications systems;
- Interoperability of devices and their functionality from many suppliers and connected by heterogeneous media;

3 Security and Resilience of Sensor Network Systems

To highlight important issues, we will follow a layered model in the style of [1], and merge in security and resilience considerations during the analysis.

3.1 Media and Pathways

None of the pathways in common use are inherently secure or resilient. Even if they are not under attack, they can be disrupted in many ways, especially if the devices are in motion. Any kind of emission can be a clue that can be used by an adversary for intercept, jamming or masquerading, e.g. by replaying. If the attack is directed at a key pathway where traffic converges then the damage could be severe unless there is redundant capability: while more pathways give more opportunity for attack, the potential for data to travel by alternative routes may increase resilience. No deployment is static and, while there are specific issues for sensor systems, especially WSN, vulnerabilities of core and access networks must also be considered, as they too evolve: pathways that were placed in carefully selected locations and replicated to give resilience may move and converge, becoming key failure points.

3.2 Physical Layer (PHY)

While it might be assumed that the small sensors typically used in WSN are more constrained to narrowband, low bit-rate, short-range operation, the increasing maturity of systems that offer very low power, very high bit rate capabilities over even shorter distances, (UWB, or emerging 60GHz band wireless Ethernet), means that many new tradeoffs can be made taking account of a multiplicity of pathways that are difficult to intercept. At other extremes we can envisage a satellite with imaging sensors with very long paths visible to many potential intruders, or an appliance plugged into mains power lines that effectively broadcasts its messages to anybody connected to the power network.

The risk of instrusion and intercept increases according to how easy it is to demodulate and decode the energy into a bit-stream, so protective measures such as changing frequency, encryption keys or waveform can increase resilience provided the algorithms are not discoverable. Some of the PHY protective measures, e.g. evasion of attack by changing slots in a multiplexing scheme, may be done better by DLC/MAC functions;

3.3 Data Link Layer and Medium Access Control (DLC/MAC)

The systems that we are interested in have a networking requirement and the DLC/MAC layer provides essential support for this – it may itself have a range of routing and relaying functions that are in effect a network layer and provide for internetworking between clusters of nodes at DLC/MAC level. Being able to use one or more links allows techniques such as network coding, cooperative relaying and directed diffusion to be deployed. A data-centric sensor network may be operated entirely within this layer.

It is usually possible to identify a location in the communications system where sensors are logically, or physically, clustered. A proxy can be located at this point to interwork between the different DLC/MAC technologies. This could be a home DSL gateway or a set-top box; the GPRS systems used for meter reading applications are architecturally very similar but on a much large scale. These proxies are a point of attack from outside and from device inside the proxied network.

Complex systems are likely to have significant vulnerabilities, allowing an attacker to subvert their operation by attacking one or more DLC/MAC segments while apparently obeying all rules of normal operation. For example, an attack may be made by a device that is marginally hyperactive and ties up system resources by repeated re-registrations, or excessive traffic at critical times. Forwarding capability, such as routing or link virtualisation can multiply the vulnerability.

The risks of intrusion are substantial because there are so many ways of collecting packets. Sessions can be recorded, edited and replayed into the network without apparent intrusion or challenge. Commercial cellular communications systems are systematically secured to prevent access except to authorized users and, once admitted, their traffic is secure at least from each other on the wireless medium.

3.4 Network Layer

If there is a requirement for end-to-end connectivity between devices then we need to be able to establish paths across namespaces under different administrations, i.e. we need a naming and addressing scheme and a routing protocol. There is a large number of such schemes, e.g. as described in [4], some of which are IP-like internetworking systems using IP routing protocols for managed and ad-hoc infrastructures and others that operate using different principles, including data-centric approaches that require no routing protocol.

The class of applications that we outlined in Section 2 has a strong end-to-end, bidirectional interaction requirement in general and it is expected that they will use IP and its internetworking models in most, if not all, of such systems. Thus they will use routing protocols and there is potential for attack to subvert the routing relationships and the paths that data will take. Much of this can be done by sending false information. Popular examples of such attacks are:

- Sinkhole attack – the attacker node sends route packets with a low hop count value or other attractive metric value to its adjacent forwarding elements, e.g. the base station at the boundary between the WSN and the access network. The attacker will thus be able to alter the content of the data flow, throw it away, or launch additional attacks (e.g. selective forwarding attack, blackhole attack, and more);
- Replay attack – the attacker records routing traffic from genuine routing nodes and uses it to create a topology that may no longer exist;
- Wormhole attacks – similar to a replay attack but done in a different part of the network;
- Sleep-deprivation – the attacker generates spurious activity that will discharge its neighbor nodes and all nodes whose paths to the base station intersect the flooded path will have difficulty communicating with the base station;

Many managed systems will protect their routing traffic by securing the associations between routing nodes. However ad-hoc systems where every node is potentially a router are more vulnerable. Significant innovation is still needed to accommodate mobility at network level: the requirement may be that a device retains its network identity wherever it is attached (as is done in Mobile IP) but we must also consider mobile networks in cars and on people.

Proxy gateways are commonly used to mediate between IP and non-IP technologies. A proxy can be located at this point to emulate end-to-end IP connectivity or perform address mappings. This can be a place to attack.

As is well-known, the IP architecture is vulnerable to crude denial-of-service attacks on exposed network addresses.

3.5 Transport Layer

The transport layer is the extension of the communications service into devices and the processes they execute. Thus it understands end-to-end delivery and relationship with its peer device(s) at remote end(s), as well as the interaction with the processes at the ends. The quality of the outcome is a tradeoff of requirements for integrity and throughput, which is an application requirement, against the resources needed to achieve them.

The trend is towards increasing resources in sensor nodes so that it is possible to support the cost of a protocol such as TCP, or features built round UDP in the application to achieve reliable delivery. Attacks on transport-layer end points (ports) are familiar to IP users, so equipping sensor nodes with TCP or UDP will expose them to attacks commonly used on computers.

3.6 Application Layer (and the Others)

We include as aspects of the application the functionality of sessions, (e.g. TLS or IPSec associations), presentation (encoding of application semantics) and middleware for discovery and node configuration, e.g. UPnP, or key-exchange and other supporting functions. All these protocols expose new information about sensor nodes (those that are capable of using them) or the proxies that implement them on the sensors' behalf.

If an intruder is able to establish connectivity at such a deep level in the system and its nodes then protection mechanisms that are supposed to prevent this have failed. This is anyway a contingency that must be anticipated: no system is perfect and its users and administrators will make mistakes or act maliciously from time to time. Maybe the measures that were provided are very simple and present only limited barriers: maybe we want to attract attackers and encourage them to give themselves away.

Depending on the application, the attack may have impacts ranging from none to catastrophic. The intruder may replay past disruptions, or create situations that appear plausible but do not exist. To achieve resilience, the system should be able to audit traffic (its originator, destination and route) and the assets connected to it. These are difficult and expensive to do, and it is inevitable that there will be a certain level of noise and interference affecting any information.

3.7 Current Approaches

As well as recent ongoing research work, e.g.[2], [3], [5] and [6], relating to intrusion detection and security in sensor networks, there are several standards that have been written to categorise security vulnerabilities and threats and define the functional capabilities to counter attacks. For example, from the ITU-T there are X.800 and X.805 that cover the larger network for end-to-end communications, and from ISO/JTC1/SC6 there is ISO29180 (currently at CD status) giving a framework for security in sensor networks. Home network security is described in ITU-T X.1111 – X.1114. Overall these standards reflect a model of the security issues split between the external networks and internal ones.

The specific vulnerabilities of a sensor network are described in ISO29180, including:

- Many nodes, but not all, lack the capability to implement security mechanisms for well-known functions. It may not be possible to use public key systems. The sensor network may be especially vulnerable to DoS attacks based on functions related to key generation and exchange;
- Compromise of nodes, when attackers evade security measures and gain access: possibly through tampering to connect directly to the electronics of the sensor; or by being able to connect to the sub-network or route via external networks to communicate with and subvert the function of the devices. Such compromises may happen because of faults in the application, interoperability failures, or poor system design: nodes that accidently make an attack may not be aware that they are behaving badly;
- Evolving deployments. The configuration of the initial deployment of the sensor network may not be known if it is scattered randomly, or it may be systematically installed and documented. A given configuration will change when sensors change position, network connectivity, or have their functionality enhanced (or reduced) or upgraded. Faults will also change the configuration, maybe transiently or permanently: loss of connectivity through lack of coverage or jamming; loss of power; and simple failure;
- Key failure points when traffic flows through a single device, such as a home gateway or a fusion node that has become the focus. This can be avoided, at a price, by exploiting redundant paths made accessible through the locally available media.

ISO29180 also identifies attackers from inside the sensor network and from networks that connect to it. The specific threats that these present include, (with reference to [5]):

- Destruction of, gaining control of, and tampering with, information or device capabilities, (hijacking);
- Intercept and disclosure of information, (eavesdropping);
- Generation of information that is incorrect (semantic disruption);
- Disruption to services, in particular to routing.

These reflect the vulnerabilities noted above, and the risks will be affected by the extent to which the sensor devices and supporting gateways are able to counter these direct threats. Disrupted routing is an especially serious threat, particularly so when an attacker can place itself at a forwarding point where it can change the pathways in addition to the threats mentioned above.

In the context of critical infrastructure, the risk assessment of the threat of intrusion must be realistic and strict. It is not likely that a separate physical core network will be installed for our family of sensor network applications: sections of the access network may however be physically separate, e.g. sensors at trackside or roadside follow the railway and highway maps. The technology for segregating traffic in a shared network using virtualization from data link layer upwards is well understood. However, an attacker could deliberately connect the infrastructures together. If routing protocol flows across this connection then the apparent topology of any of the involved infrastructures could change and traffic would mix and flow in unexpected ways. Self-organising applications, that discover and configure devices and functionality without user intervention might enroll inappropriate functions or other attacking nodes, and thereby cause unwanted behaviour. A person's home in which telecare and energy management applications coexist is exactly such an interconnection point, and one that would be expected to exist.

4 Coexistence, Interworking and Interoperability

Because multiple applications, services and devices will share resources and infrastructure to some extent, it is essential that they do so without conflict. Additionally, it is certain that communications systems will become more heterogeneous, not less, especially where wireless technologies are used. Thirdly, there is already a wide diversity of standards in sensor network domains. These standards come from a range of bodies – the IEEE, the ITU, ISO, ETSI, and the IETF – and may fulfil the same function in different ways. Some are regional or sector specific even if they have the status of International Standards. This diversity is especially apparent where bodies traditionally concerned with professional ICT equipment (the IEEE) or telecommunications (the ITU, ETSI) are developing specifications for sensor systems or machine-to-machine communication to be used by consumers in general.

The presence of multiple processes active in the same space, physical or electronic, leads to failures of interoperability. This is a term that is widely used and is understood in different ways: it is more than just the ability to communicate and exchange bits across a collection of technology-specific pathways. The bits must be combined and formatted as structured data; the data must be comprehended as information independent of representation; and the information must be used and acted upon in a consistent way to achieve real effects. However, the term is used in all these contexts and many others, e.g. the rules of working between the police, fire and ambulance services, so our interpretation must be clearly stated.

In managing the solutions to interoperability problems, we make a distinction between aspects that are mainly technical and those that are concerned with processes outside ICT and electronic domains of sensing and actuation, e.g. the management of a domestic heating system to an occupant's requirements, taking account of the weather and the heating cycle of the building. Here we are interested primarily in the former. The technical aspects of interoperability should be uniform and consistent for all processes so that the ambition of sharing infrastructure and resources can be achieved.

At a technical level, we can express three requirements, each of which has an interoperability aspect:

- Co-existence - where different systems can operate in the same environment without hindering each others' operation or otherwise conflicting: e.g. a home wireless security system using Zigbee, a WiFi local area network, and a Bluetooth telecare service. All occupy the same ISM spectrum and will potentially interfere with each other but they are separate applications involving interoperable devices;

- Interworking - where different technologies are connected together to transfer data end-to-end. It is primarily a technical solution encompassing connectors, protocols, bridges, etc. An example is where the home security system above is connected to a PC monitoring application using the WiFi network to transfer the data between the security system and an external web application. At some point the different communications systems come together at one or more gateways and information can flow between them;
- Interoperability is where different application functions interoperate with each other: this adds business rules, processes, security provisions, etc. that enable applications to be joined together and to use devices of any provenance. The example here is the home wireless security system being controlled and monitored remotely using a separate web application, possibly sending alerts to the owner's mobile telephone or, locally, to the TV set.

The new challenge for interoperability is to ensure that the three requirements are met for systems of variable structure and population; changed and evolved by their users, who will generally be non-professional consumers lacking technical expertise; operating distributed algorithms and protocols with a significant level of machine-to-machine autonomy; as well as executing a range of applications, which may change from time to time, sharing resource, devices and infrastructure.

We have seen already, in section 3, how this variability impacts on security and resilience. Let us now look at it from a specific industry and standardization viewpoint.

4.1 Current Approaches

One area where sensor networks are likely to be widely deployed is the home, e.g. for management of resource consumption (electricity, gas and water), telecare, and a wide range of personal applications, such as entertainment, security, or comfort control. These are termed collectively Home and Building Electronic Systems: HBES.

There are already many standards established for the communications systems supporting HBES: IEEE 11073 for healthcare devices, EN50090 (CENELEC TC205) and EN14908 (CENELEC TC247) for control and communication. There are several activities in ETSI (the M2M group), ITU-T (e.g. G.hn and G.cx, or the G.6690 recommendation), and ISO/SC25/WG1 that have a direct impact on future directions. Where HBES interact with other systems, a range of ICT standards (e.g. UPnP) or IP protocols are used.

Because of the diversity of solution and the large number of legacy deployments, agreement on a single specification or standard is unlikely, so the need for an interoperability solution meeting at least the three requirements outlined above is a priority. Even this is contentious: maintaining interoperability even for devices implementing the same standard has proved difficult, so what prospect of success can be expected when multiple systems are interconnected?

To begin to address this problem in the light of the challenge posed by highly dynamic systems. CENELEC TC205 approved in July 2008 the formation of a Workshop that will deliver an Agreement that defines an Interoperability Framework and requirements for complying with it. Such an Agreement is voluntary and will be developed into a collection of mandatory conformance requirements in the form of a CENELEC Technical Specification. The Workshop is close to finalizing the text of the Agreements, which has the following key points:

- A categorization of Interoperability Levels, as shown in Table 1. This associates coexistence, interworking and interoperability between dissimilar systems with levels 1, 2 and 3, reflecting the current state of the art. Levels 4, 5 and 6 look into the future to highlight the greater dynamics of HBES systems, the prevalence of machine-to-machine autonomy at local and remote level, and the wider range of applications that will reach into the home;
- A categorization of middleware functions needed to support the formation of applications at level 4 and above: device discovery, application configuration, and management. A survey of the 17 or so contemporary standards in the HBES domain showed that these three groups of functions were provided by all of them in isolation, even though the way they work varies in detail;
- A set of conformance requirements placed upon devices, (sensors, actuators, gateways/routers, and the controlling application components) to enable them to state compliance with the framework of levels and functions, and identify the objects that they implement;
- Specific provision for security and measures to enhance resilience following the models of section 3 above;
- A formal specification of the structure and required content of an Interoperability Implementation Conformance Statement to be applied to products regardless of their provenance and the standard(s) that they implement.

Table 1. Interoperability Levels

0	A single system of supplier-defined structure built from devices using a single HBES specification and locally defined interoperability verified by the supplier for one or more application domains. No assurance of coexistence is provided.
1	A Level 0 system.operating across one or more application domains Verified coexistence is required.
2	Multiple Level 1 systems that interwork to exchange information and interoperate across specification and application domains verified by the suppliers using conformance specifications.agreed by each HBES specification used.
3	As Level 2, and the interoperability is verified with respect to international standards applicable to the HBES specifications used in the system.
4	As Level 3, but conforming to IFRS so that the applications and devices can be installed, managed and changed during the operation of the system by a qualified installer.
5	As Level 4, and changes of application and devices will be done automatically.
6	As level 5, and with remote management, diagnostics and maintenance. (automatic installation, operation and support).

An assurance of interoperability end-to-end between devices and application elements is an important complement to measures taken to ensure quality and grade of service of the network and security of its operation. While the CENELEC Workshop Agreement is a starting point in achieving this assurance, it is likely to take some time before it becomes acceptable as a Technical Specification and mandatory.

5 Conclusions and Future Work

The work reported in this paper has considered the security, resilience and interoperability issues that will be important in fulfilling expectations of quality of service, availability and integrity of sensor network applications that will form part of the critical infrastructure of future society.

This infrastructure, and the resources and devices connected to it, will be shared by many applications executing on behalf of millions of people, at home and on the move, and involve a multiplicity of services in the home, at work and in public spaces. Several issues remain to be addressed, related to the scale in population and diversity of behaviour:

- Integration of very large numbers of sensors – how much, or how little, state must be stored to maintain connectivity, implement effective sharing, record usage, and ensure security;
- Unusual traffic distributions triggered by human activity or the environment, or autonomously between machines, with interaction occurring at machine timescales. These could be an indication of attack, or maybe just unexpected behaviour;
- Managing connectivity and presence of a large number of small networks, fixed and mobile;
- Developing a formal model of interoperability as support for greater resilience and security.

Acknowledgement

The author is grateful to ENISA and TAHI (The Application Home Initiative) for partial support in doing the work reported here.

References

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks 38, 393–422 (2002)

[2] Braun, T., Danzeisen, M.: Secure Mobile IP Communication, Uni. Bern internal report

[3] Anand, M., Cronin, E., et al.: Sensor Network Security: More Interesting Than You Think. In: Proceedings of HotSec 2006, Usenix Workshop on Hot Topics in Security (2006)

[4] Karaki, J.N., Kamal, A.E.: Routing Techniques in Wireless Sensor Networks: A Survey. IEEE Wireless Communications, 6–28 (December 2004)

[5] Martynov, D., Roman, J., Vaidya, S., Huirong, F.: Design and implementation of an intrusion detection system for wireless sensor networks. In: IEEE International Conference on Electro/Information Technology, pp. 507–512 (2007)

[6] Mitrokotsa, A., Karygiannis, A.: Intrusion Detection Techniques in Sensor Networks. In: Wireless Sensor Network Security. Cryptology and Information Security Series, vol. 1, pp. 251–272. IOS Press, Amsterdam (April 2008), ISBN 978-1-58603-813-7

Wide–Weak Privacy–Preserving RFID Authentication Protocols

Yong Ki Lee[1], Lejla Batina[2,3], Dave Singelée[2], and Ingrid Verbauwhede[2]

[1] Samsung Electronics Research and Development, South-Korea
`yklee93@kg21.net`
[2] IBBT – COSIC, Katholieke Universiteit Leuven, Heverlee, Belgium
`{firstname.lastname}@esat.kuleuven.be`
[3] Digital Security group, Radboud University Nijmegen, Nijmegen, The Netherlands
`lejla@cs.ru.nl`

Abstract. The emergence of pervasive computing devices such as RFID tags raises numerous privacy issues. Cryptographic techniques are commonly used to enable tag-to-server authentication while protecting privacy. Unfortunately, these algorithms and their corresponding implementations are difficult to adapt to the extreme conditions implied by the use of RFID. The extremely limited budget for energy and area do not allow the use of traditional cryptography.

In this paper, we address the risk of tracking attacks in RFID networks. Many lightweight protocols have been proposed so far that are founded on both, private- and public-key cryptosystems. We give an overview of existing solutions and discuss the latter ones in more detail. The solutions we advocate in this paper rely exclusively on Elliptic Curve Cryptography (ECC). We describe several authentication protocols that have different computational demands and accordingly different security features. To the best of our knowledge, these protocols are the first ECC-based authentication protocols which offer privacy protection against a wide-weak attacker. Compared to other RFID schemes proposed in the literature, our protocols remain light-weight in terms of area and computation time, while still achieving the required security and privacy properties.

Keywords: Authentication Protocol, Privacy, Tracking Attack, Elliptic Curve Cryptography, RFID.

1 Introduction

RFID tags, smart labels, sensor nodes are involved in the distributed, wireless, mobile computing revolution, which moves information gathering and processing into the human environment. This evolution has a profound impact on security. Traditional security applications, such as secure gateways, virtual private networks (VPNs), *etc.* focus on protecting the communication channels between computers against attacks. This protection is based on security protocols

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 254–267, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

and cryptographic algorithms running on the powerful processors of physically-protected servers. In an environment of small embedded, distributed, wireless connected devices, this assumption is not valid anymore. The embedded device itself is vulnerable to attacks, and a hacker will select the method of attack that breaks the weakest link in an entire system, including the embedded device as well as its communication channel. On top, the embedded device has limited computing and energy resources, and security is expensive (in terms of extra processing, memory, energy and development cost).

Due to the wide-spread of RFID tags, several security and privacy issues arise. Privacy addresses the resistance against unauthorized identification, tracking or linking tags. More in detail, one typically wants to achieve *untraceability*, in which the (in)equality of two tags must be impossible to determine. Several theoretical models to address the privacy of RFID systems have been proposed in the literature [1,15,21,27]. To define privacy in this paper, we import two characteristics of attackers from the theoretical framework of Vaudenay [27]: *wide* (or *narrow*) attackers and *strong* (or *weak*) attackers. If an attacker has access to the result of the verification (accept or reject) in a server, he is a *wide* attacker. Otherwise he is a *narrow* attacker. If an attacker is able to extract a tag's secret and reuse it, he is a *strong* attacker. Otherwise he is a *weak* attacker. A *wide-strong* attacker is hence the most powerful. If a protocol is untraceable against a *wide-strong* attacker, we call the protocol *wide-strong* privacy-preserving.

Operational and security requirements for RFID systems include system scalability, anonymity and anti-cloning. Obtaining all these properties presents a substantial research challenge due to rigid constraints in area, memory, power, *etc.* A common work-around is to use protocols using symmetric key cryptographic algorithms. However, the symmetric key based solutions cannot meet all the requirements and it was shown in several publications that public-key cryptography (PKC) is a must in order to have strong security for embedded applications.

In this paper, we present two authentication protocols that use public-key cryptography to achieve the required security and privacy goals. The protocols rely exclusively on the use of Elliptic Curve Cryptography (ECC) and are, to the best of our knowledge, the first ECC-based RFID authentication protocols that are both narrow-strong and wide-weak privacy preserving.

The remainder of the paper is organized as follows. In Section 2, related work is reviewed. We discuss our authentication protocols in detail in Sect. 3. We conclude our paper in Section 4.

2 State of the Art

Various RFID authentication protocols have been proposed in the literature. In the beginning the main efforts were on designing solutions that rely exclusively on private-key (also called symmetric-key) cryptography. One of the first was the work of Feldhofer [11] that proposed a challenge-response protocol based on the AES block-cipher. Toiruul and Lee presented an mutual authentication algorithm based on AES [25]. Of other notable solutions for authentication protocols we mention here the HB^+ protocol [16] that was presented as an extremely cheap solution but still secure against active adversaries. It meets even the cost requirements for the tags of 5-10 cents range. Other variants of HB followed, as a result of attacks that appeared, such as the work of Gilbert *et al.* [13], and the most recent one is of Frumkin and Shamir [12]. As a fix a new protocol called HB^{++} from Bringer *et al.* [5] was proposed. HB^{++} is claimed to be secure against man-in-the-middle attacks (as in [13]) but it requires additional secret key material and universal hash functions to detect the attacks. In the follow-up work Bringer and Chabanne [4] proposed a new HB^+ variant (so-called Trusted-HB) that builds upon Krawczyk's hash-based authentication schemes using special LFSR constructions (via Toplitz matrix).

A novel authentication and forward private RFID protocol is proposed by Berbain *et al.* [3]. The protocol is using pseudo-random number generators and universal hash functions as basic building blocks, which makes it suitable for low-footprint solutions. The security of their scheme is proven in the standard model but it remains unclear whether it can withstand physical attacks (*i.e.* tampering with the tag, such that the tag can be cloned).

The main reason why most work focussed on symmetric-key solutions lies in the common perception of public-key cryptography being too slow, power-hungry and too complicated for such low-cost environments. However, recent works proved this concept to be wrong, as for example the smallest published ECC implementations [20,14] consume less area than any known secure cryptographic hash function (*e.g.*, the candidate algorithms proposed in the SHA-3 competition [22]). One alternative is therefore, to pursue protocols that use only public-key cryptography. In [18], it is shown that some conventional public-key based authentication protocols, such as the Schnorr protocol [24] and the Okamoto protocol [23], do not resist tracking attacks. Accordingly, the EC-RAC (Elliptic Curve Based Randomized Access Control) protocol has been proposed to address the established privacy threat. However, in [6,8], it is shown that EC-RAC is also vulnerable to tracking attacks and replay attacks, and in addition [6], the randomized Schnorr protocol has been proposed as an alternative for EC-RAC. This protocol is narrow-strong privacy preserving, but does not offer privacy protection against a wide-weak attacker. EC-RAC has been gradually revised in [19,17]. However, Fan *et al.* [10] have shown that the most recent version of EC-RAC [17] is not wide-weak privacy preserving.

In addition, we also mention RFID authentication protocols that are based on Physical Unclonable Functions (PUFs) [26]. It was shown that those solutions can also prevent counterfeiting in on-line and off-line scenarios and are feasible for active tags. However, they require both private-key and public-key algorithms.

Note that in this paper, we only consider RFID authentication protocols on the logical level. Danev *et al.* [7] have shown that one can also identify RFID tags with a high accuracy from a small distance (*e.g.*, less than 1 meter), based on their physical-layer fingerprints. This technique automatically enables tag-to-server authentication. However the downside of this solution is the requirement that the distance between RFID tag and reader should be small, in order to have a high accuracy. On the other hand, allowing a large distance between reader and tag, as is the case for RFID authentication protocols on the logical level, gives more freedom to the attacker and hence makes him more powerful (*e.g.*, it becomes easier to carry out man-in-the-middle attacks).

In the next Section of this paper, we focus more in detail on authentication protocols based on public-key cryptography, more specifically on ECC.

3 ECC-Based Untraceable RFID Authentication Protocols

3.1 System Parameters

Table 1 shows the notation that is used in the rest of this paper. We denote P as the base point, and y and $Y(=yP)$ are the server's private-key and public-key pair, where yP denotes the point derived by the point multiplication operation on the Elliptic Curve group. x_1 and $X_1(=x_1P)$ are a tag's private-key and public-key pair. We will denote these values as the (secret) *tag's ID* and the *tag's ID-verifier* respectively. One should note, although the name suggests that it can be publicly known, that the public-key of the tag (i.e. the ID-verifier) should be kept secret in the server. Revealing this key causes tracking attacks.

Table 1. System Parameters

System Parameters	y : Server's private-key
	$Y(=yP)$: Server's public-key
	x_1 : Tag's ID
	x_2 : Tag's password (Pwd)
	$X_1(=x_1P)$: Tag's ID-verifier
	$X_2(=x_2P)$: Tag's Pwd-verifier
	P : Base point in the EC group
	n : Prime order of P
ID-transfer	y, X_1, P, n (Server)
	x_1, Y, P, n (Tag)
ID&Pwd-Transfer,	y, X_1, x_1, X_2, P, n (Server)
	x_1, x_2, Y, P, n (Tag)

3.2 Narrow vs. Wide Privacy

Several solutions using public-key algorithms have been proposed in order to protect RFID tags from tracking attacks. Since they are only narrow-strong privacy-preserving, they are all vulnerable to man-in-the-middle attacks carried out by a wide attacker. Let us illustrate this with the ID-transfer scheme of the revised EC-RAC protocol [19], which is shown in Fig. 1.

Deursen and Radomirović [9] demonstrated a man-in-the-middle attack on this scheme in [9], as shown in Fig. 2. The attack is performed by manipulating

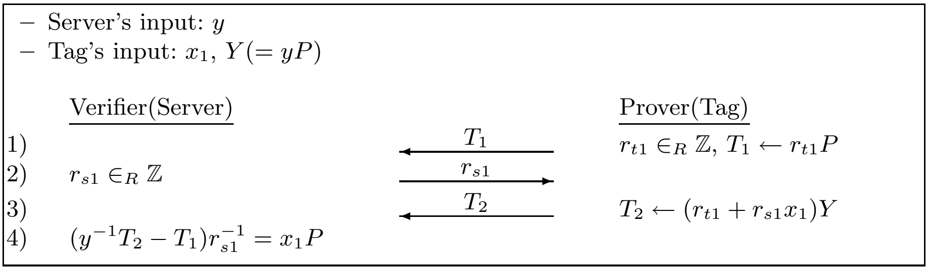

– Server's input: y
– Tag's input: x_1, $Y(= yP)$
Verifier(Server)
Prover(Tag)
1)
T_1
$r_{t1} \in_R \mathbb{Z}$, $T_1 \leftarrow r_{t1}P$
2)
$r_{s1} \in_R \mathbb{Z}$
r_{s1}
3)
T_2
$T_2 \leftarrow (r_{t1} + r_{s1}x_1)Y$
4)
$(y^{-1}T_2 - T_1)r_{s1}^{-1} = x_1P$

Fig. 1. ID-Transfer Scheme [19]

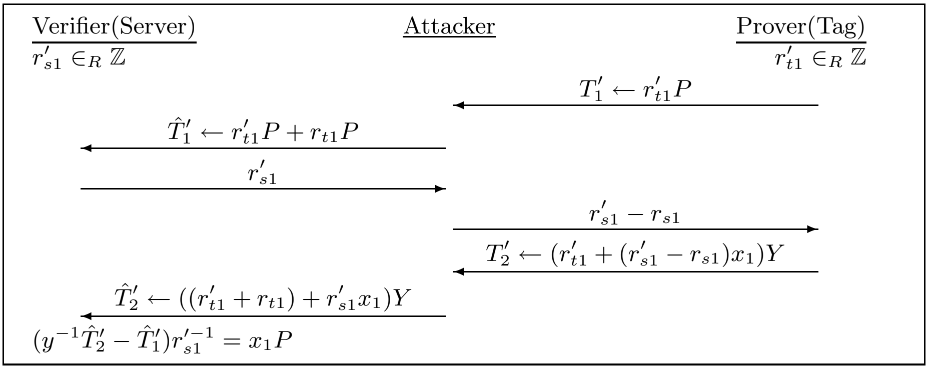

Verifier(Server)
Attacker
Prover(Tag)
$r'_{s1} \in_R \mathbb{Z}$
$r'_{t1} \in_R \mathbb{Z}$
$T'_1 \leftarrow r'_{t1}P$
$\hat{T}'_1 \leftarrow r'_{t1}P + r_{t1}P$
r'_{s1}
$r'_{s1} - r_{s1}$
$T'_2 \leftarrow (r'_{t1} + (r'_{s1} - r_{s1})x_1)Y$
$\hat{T}'_2 \leftarrow ((r'_{t1} + r_{t1}) + r'_{s1}x_1)Y$
$(y^{-1}\hat{T}'_2 - \hat{T}'_1)r'^{-1}_{s1} = x_1P$

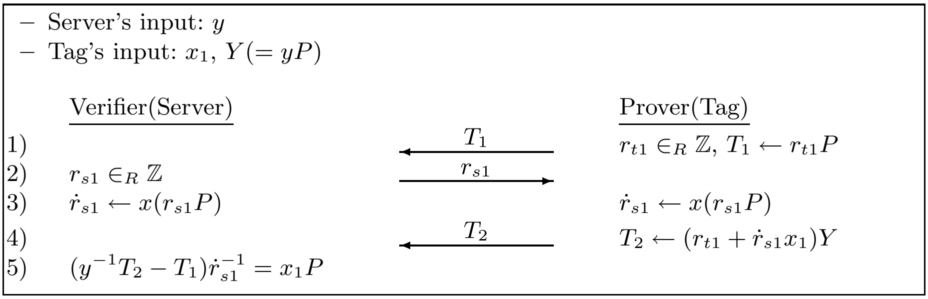
Fig. 2. Illustration of a Man-in-the-Middle Attack on the Revised EC-RAC [9]

messages exchanged in previous protocol instances. A similar problem arises in the randomized Schnorr protocol [6] and the password-transfer scheme of the most recent version of EC-RAC [17]. No solution founded on public-key cryptography had yet been proposed that is both narrow-strong and wide-weak privacy preserving.

3.3 New ID-Transfer Scheme

In this paper, we present two RFID authentication protocols which are both narrow-strong and wide-weak privacy preserving. The first authentication protocol is an ID-transfer scheme, which allows the tag to demonstrate its knowledge of its secret ID. The second authentication protocol combines two sub-modules: the ID-transfer scheme and a password-transfer (shortly, Pwd-transfer) scheme. Both RFID authentication protocols fulfill a specific set of privacy and security requirements.

Protocol Description. To prevent man-in-the-middle attacks carried out by a wide attacker, one can use a cryptographic hash function to introduce non-linearity, as noted in [9]. However, this requires additional hardware to implement the cryptographic hash function, which is undesirable due to the limited hardware resources of a tag. To avoid this, we suggest to introduce the required non-linearity by reusing EC-operations. Our proposed ID-transfer scheme is shown in Fig. 3, where $\dot{r}_{s1} = x(r_{s1}P)$ denotes the x-coordinate of $r_{s1}P$. To ensure valid authentication claims, the value r_{s1} should be different from zero and the order of P on the elliptic curve. The computation of the x-coordinate of $r_{s1}P$ only introduces a slight increase in the cost: the server and the tag need to perform one extra EC point multiplication.



- Server's input: y
- Tag's input: x_1, $Y (= yP)$

	Verifier(Server)		Prover(Tag)
1)		$\xleftarrow{T_1}$	$r_{t1} \in_R \mathbb{Z}$, $T_1 \leftarrow r_{t1}P$
2)	$r_{s1} \in_R \mathbb{Z}$	$\xrightarrow{r_{s1}}$	
3)	$\dot{r}_{s1} \leftarrow x(r_{s1}P)$		$\dot{r}_{s1} \leftarrow x(r_{s1}P)$
4)		$\xleftarrow{T_2}$	$T_2 \leftarrow (r_{t1} + \dot{r}_{s1}x_1)Y$
5)	$(y^{-1}T_2 - T_1)\dot{r}_{s1}^{-1} = x_1P$		

Fig. 3. ID-Transfer Scheme Resistant to Man-in-the-Middle Attacks (Protocol 1)

Protocol Analysis. We analyze our ID-transfer scheme in two phases: first the security analysis and then the privacy analysis. The security analysis is performed by reducing the proposed protocol to the Schnorr protocol. Reducing a protocol means that we modify a protocol to give an attacker more adversarial power (or more information). Therefore, the original protocol will be at least as secure as the reduced protocol (shown in Fig. 4). Since the security of the Schnorr protocol is proven in [2], the reduction concludes the proof. For the privacy analysis, we first show its narrow-strong privacy and then demonstrate that the protocol also offers privacy protection against a wide-weak attacker.

• **Security Analysis:** We modify the proposed protocol such that the server transmits the following values in Steps 2) and 3) in Fig. 3.

$$r_{s1},\ \dot{r}_{s1} \tag{1}$$

Since the mapping from r_{s1} to $\dot{r}_{s1}$ (the x-coordinate of $r_{s1}P$) is deterministic, even if the server transmits both the values r_{s1} and $\dot{r}_{s1}$ to a tag, the protocol derived is equivalent to the former one.

Now we reduce the protocol by dropping r_{s1}, so the server only transmits $\dot{r}_{s1}$ (as is shown in Step 3 of Fig. 4). Since r_{s1} is only used to derive $\dot{r}_{s1}$, $\dot{r}_{s1}$ is sufficient information for the tag to produce a response. However, by dropping r_{s1}, an attacker gets more freedom to manipulate $\dot{r}_{s1}$, since he does not need to derive it from r_{s1}. In other words, in this case a tag does no longer know if the

	Verifier(Server)		Prover(Tag)
1)		$\xleftarrow{T_1}$	$r_{t1} \in_R \mathbb{Z}$, $T_1 \leftarrow r_{t1}P$
2)	$r_{s1} \in_R \mathbb{Z}$		
3)	$\dot{r}_{s1} \leftarrow x(r_{s1}P)$	$\xrightarrow{\dot{r}_{s1}}$	
4)	$T_2 \leftarrow vY$	$\xleftarrow{v}$	$v \leftarrow r_{t1} + \dot{r}_{s1}x_1$
5)	$(y^{-1}T_2 - T_1)\dot{r}_{s1}^{-1} = x_1P$		

Fig. 4. Reduced Scheme from Fig. 3

received challenge is an actual output of the one-way function of the EC point multiplication.

Another reduction is performed in Step 4. A tag transmits $v(= r_{t1} + \dot{r}_{s1}x_1)$ instead of $T_2(= (r_{t1} + \dot{r}_{s1}x_1)Y)$. Since given v and Y, T_2 can be easily computed, an attacker gets extra information by eavesdropping v (instead of T_2) in this reduced protocol.

The reductions described above result in a reduced protocol (Fig. 4) where the exchanged messages are equivalent to the Schnorr protocol. Hence, one can conclude that our proposed protocol can be reduced to the Schnorr Protocol.

- **Narrow-Strong Privacy:** This proof can be done similarly to the proof in [19]. The three messages exchanged in the protocol are:

$$r_{t1}P,\ r_{s1},\ (r_{t1} + \dot{r}_{s1}x_1)Y \tag{2}$$

$r_{t1}P$ is a random point generated by a tag, and r_{s1} a random value that is possibly controlled by an attacker. These two messages themselves include no information about a tag. The last message can be considered as an addition of two EC points as follows:

$$(r_{t1} + \dot{r}_{s1}x_1)Y = r_{t1}yP + \dot{r}_{s1}x_1yP \tag{3}$$

Assuming that the Decisional Diffie-Hellman problem is hard, the first point $r_{t1}yP$ is a random secret shared between the server and a tag upon the transmission of $r_{t1}P$. Therefore, the EC point addition can be considered as a one-time pad with a one-time secret key $r_{t1}yP$, which means that $(r_{t1}+\dot{r}_{s1}x_1)Y$ is nothing more than a random point for an attacker. Note that there is no effect from r_{s1} on the one-time pad, which is the only message that could possibly be controlled by an attacker. Therefore, the proposed protocol is narrow privacy-preserving.

Another thing we can note is that the secret of the one-time pad, $r_{t1}yP$, does not include any information about a tag. It only contains the public key of the server and random data which is unknown to the attacker. It does not depend on the identity of the tag. Therefore, even if an attacker knows the secret key of a tag, x_1, it doesn't help for interpreting the encrypted message. So, the protocol is narrow-strong privacy-preserving.

• **Wide-Weak Privacy:** For a wide attacker, there is one-bit extra information compared to a narrow attacker: the decision of the server whether to accept a tag or not. This extra bit of information can be used by a wide-weak attacker to perform a tracking attack. The goal of this attacker is to determine if two sets of protocol instances originate from the same tag. One of these sets contains authentic messages from the past. Let us denote the source (*i.e.* the tag) of these messages by A. The other set contains the responses of a tag B. The tracking attack is successful when the attacker can determine the (in)equality of the two tags A and B with a probability significantly larger than $\frac{1}{2}$.

This (in)equality can be checked by verifying if both protocol instances use the same secret value x_1 (this is the only value used in the protocol which is tag-dependent). This value is exclusively used to compute T_2. The message T_1 only depends on a random number r_{t1} generated by the tag. Note that a wide-weak attacker does not know the secret x_1 and the random values r_{t1}. Since the decisional Diffie-Hellman problem is assumed to be hard, the attacker cannot extract the value x_1 out of the protocol message T_2. The only strategy that an attacker can carry out, is construct a message pair (T'_1, T'_2), using messages $(T_{1,i}, T_{2,i})$ [1], in such a way that T'_2 will only be accepted by the server if tag A equals tag B (*i.e.* if the same secret value x_1 is used in both sets of protocol instances).

Without loss of generality, let us assume that tag A equals tag B. When carrying out the ID-transfer scheme, the server will send the challenge r'_{s1}, and receive the messages (T'_1, T'_2) from the attacker. It will accept these messages if the following equation hold:

$$T'_2 = yT'_1 + \dot{r}'_{s1} x_1 Y \tag{4}$$

Note that the attacker does not know the secret key y. However, the attacker can exploit the linear property of addition on an elliptic curve to construct a valid pair (T'_1, T'_2). The attacker first chooses a linear function $f()$ and computes T'_1 as follows:

$$T'_1 = f(\bigcup_i (T_{1,i})) \tag{5}$$

In the equation above, $\bigcup_i (T_{1,i})$ denotes a cluster of messages $T_{1,i}$, selected by the attacker, from both sets of protocol instances. Next, the attacker can compute T'_2 as follows:

$$T'_2 = f(\bigcup_i (T_{2,i})) \tag{6}$$

In the equation above, $\bigcup_i (T_{2,i})$ denotes a cluster of messages $T_{2,i}$, selected by the attacker, from both sets of protocol instances. Note that $T_{1,i}$ and $T_{2,i}$ have to originate from the same protocol instance. *I.e.*, the following relation holds:

$$T_{2,i} = yT_{1,i} + (\dot{r}_{s1,i} x_1)Y \tag{7}$$

---

[1] The index i denotes that the cluster of messages can originate from both sets of protocol instances.

When combining Eqs. (5), (6) and (7), one can notice that the first term of Eq. (4) will always be equal to yT_1' due to the linear property of the function $f()$. The second term in the addition is also correct if the following equation holds:

$$\dot{r'}_{s1} = f(\bigcup_i (\dot{r}_{s1,i})) \tag{8}$$

Since the attacker has to send the message T_1' to the server before it receives the challenge r_{s1}', the attacker has to select the set of protocol instances of tag A and the function $f()$ in advance. After having received the challenge, the attacker can only control the challenge r_{s1} that it sends to tag B. The attacker hence has to select a challenge r_{s1} such that Eq. (8) holds. However, since point multiplication on an elliptic curve is assumed to be a one-way function, an arbitrary control of $x(r_{s1}P)$ is infeasible. As a result, an attacker cannot construct the message pair (T_1', T_2') using Eq. (5) and Eq. (6). Note that when a non-linear function $f()$ would be used, the first term of Eq. (4) never holds, and the attack will hence not work.

Since a wide-weak attacker cannot carry out the tracking attack described above, the ID-transfer scheme (Protocol 1) is wide-weak privacy-preserving.

3.4 New Pwd-Transfer Scheme

After the ID-transfer scheme, one can carry out a Pwd-transfer scheme. This offers increased security protection (we will come back to this issue later in the paper). By performing the ID-transfer scheme, the server will obtain the ID-verifier X_1. Using this verifier, the server can look up the tag's information (x_1 and X_2) in a local database. We hence assume that the server knows x_1 and X_2 during the execution of the Pwd-transfer scheme.

Protocol Description. Let us first focus on the Pwd-transfer scheme itself. Its design concept is completely equivalent to the ID-transfer scheme, as is shown in Fig. 5. After generating r_{t1} and T_1, a tag transmits T_1 to the server. Then, the server responds with a random challenge r_{s1} (not equal to zero or the order of P on the elliptic curve), which is used to derive $\dot{r}_{s1}$. Finally, after having received the message T_2 from a tag, the server derives $X_2(= x_2P)$ and verifies it by comparing it with the stored Pwd-verifier in the database.

Protocol Analysis. If one compares the Pwd-transfer scheme and the ID-transfer scheme, one can notice that the only difference is the message T_2, where $(r_{t1} + \dot{r}_{s1}x_1x_2)Y$ is used instead of $(r_{t1} + \dot{r}_{s1}x_1)Y$. In this message, the secret identity x_1 is used to mask the secret password x_2. One can represent T_2 as follows:

$$(r_{t1} + \dot{r}_{s1}x_1x_2)Y = (r_{t1} + \dot{r}_{s1}x_3)Y \tag{9}$$

Since the secret ID x_1 and the secret password x_2 are two independent numbers, their product can be substituted by the secret value x_3. The Pwd-transfer scheme

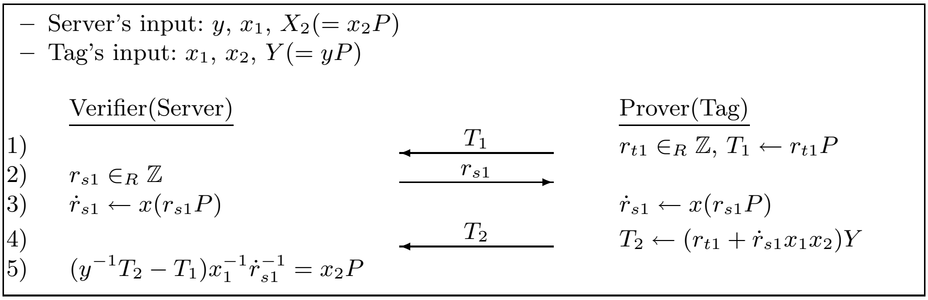

– Server's input: y, x_1, $X_2(= x_2P)$
– Tag's input: x_1, x_2, $Y(= yP)$
Verifier(Server)
Prover(Tag)
1) $r_{t1} \in_R \mathbb{Z}$, $T_1 \leftarrow r_{t1}P$
T_1
2) $r_{s1} \in_R \mathbb{Z}$
r_{s1}
3) $\dot{r}_{s1} \leftarrow x(r_{s1}P)$
$\dot{r}_{s1} \leftarrow x(r_{s1}P)$
4) $T_2 \leftarrow (r_{t1} + \dot{r}_{s1}x_1x_2)Y$
T_2
5) $(y^{-1}T_2 - T_1)x_1^{-1}\dot{r}_{s1}^{-1} = x_2P$

Fig. 5. Pwd-Transfer Scheme Resistant to Man-in-the-Middle Attacks

can hence be considered as an ID-transfer scheme with secret identity x_3. As a result, the Pwd-transfer scheme is completely equivalent to the ID-transfer scheme. Therefore, the Pwd-transfer scheme has the same security and privacy properties as the ID-transfer scheme: it is as least as secure as the Schnorr protocol, and is both narrow-strong and wide-weak privacy-preserving.

3.5 ID&Pwd-Transfer Scheme

As described above, it is interesting to combine the ID-transfer scheme with the Pwd-transfer scheme. If only the ID-transfer scheme is used for authentication, the security level could be reduced if the number of tags is extremely large. Since the authentication is performed by checking the existence of a derived ID-verifier in the server's database, the probability that an attacker randomly generates an ID that also appears in the server's database (and hence will be accepted by the server during the protocol) increases when the number of tags grows. In applications where this would cause security problems, one can use an RFID authentication protocol that combines the ID-transfer scheme with the Pwd-transfer scheme. We will now discuss this more in detail.

Protocol Description. The proposed ID-transfer scheme (Fig. 3) and Pwd-transfer scheme (Fig. 5) can be combined in two different ways: Fig. 6 (vulnerable to tracking attacks) and Fig. 7 (Protocol 2).

Security and Privacy Analysis. Let us now analyze both combinations. In the protocol shown in Fig. 6, the same random number r_{t1} is used for both the ID-transfer scheme and the Pwd-transfer scheme. While this reduces the computation load in a tag, this also causes a vulnerability to tracking attacks. An eavesdropper can track the tag by observing the exchanged messages. This can be seen in the following computation:

$$\begin{aligned} & \dot{r}_{s1}^{-1}(T_2 - T_3) \\ &= \dot{r}_{s1}^{-1}((r_{t1} + \dot{r}_{s1}x_1)Y - (r_{t1} + \dot{r}_{s1}x_1x_2)Y) \\ &= \dot{r}_{s1}^{-1}(\dot{r}_{s1}x_1 - \dot{r}_{s1}x_1x_2)Y \\ &= (x_1 - x_1x_2)Y \end{aligned} \tag{10}$$

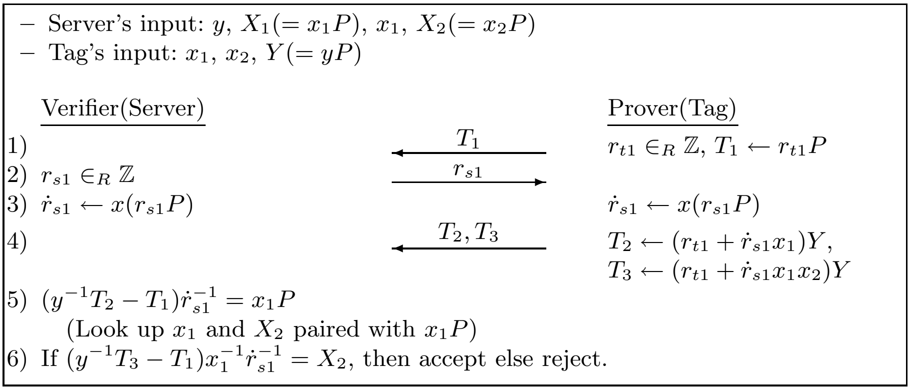

– Server's input: y, $X_1(=x_1P)$, x_1, $X_2(=x_2P)$
– Tag's input: x_1, x_2, $Y(=yP)$
Verifier(Server)
Prover(Tag)
1) $r_{t1} \in_R \mathbb{Z}$, $T_1 \leftarrow r_{t1}P$
T_1
2) $r_{s1} \in_R \mathbb{Z}$
r_{s1}
3) $\dot{r}_{s1} \leftarrow x(r_{s1}P)$
$\dot{r}_{s1} \leftarrow x(r_{s1}P)$
4) $T_2 \leftarrow (r_{t1} + \dot{r}_{s1}x_1)Y$,
$T_3 \leftarrow (r_{t1} + \dot{r}_{s1}x_1x_2)Y$
T_2, T_3
5) $(y^{-1}T_2 - T_1)\dot{r}_{s1}^{-1} = x_1P$
(Look up x_1 and X_2 paired with x_1P)
6) If $(y^{-1}T_3 - T_1)x_1^{-1}\dot{r}_{s1}^{-1} = X_2$, then accept else reject.

Fig. 6. Authentication protocol vulnerable to tracking attacks

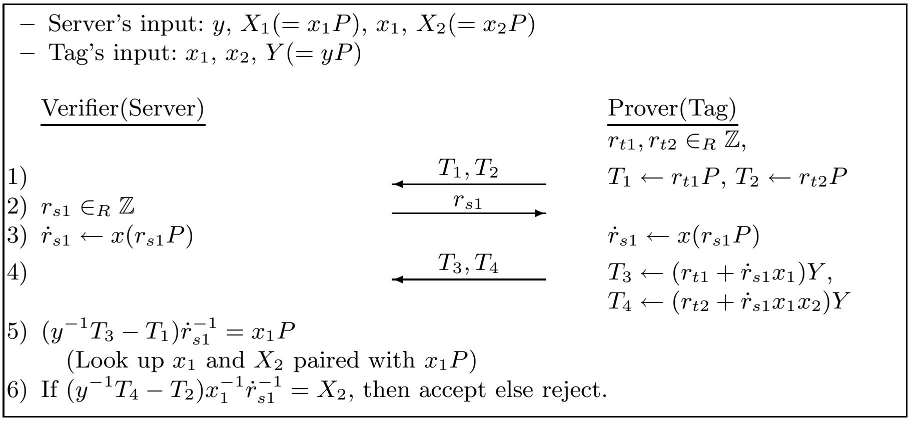

– Server's input: y, $X_1(=x_1P)$, x_1, $X_2(=x_2P)$
– Tag's input: x_1, x_2, $Y(=yP)$
Verifier(Server)
Prover(Tag)
$r_{t1}, r_{t2} \in_R \mathbb{Z}$,
1) $T_1 \leftarrow r_{t1}P$, $T_2 \leftarrow r_{t2}P$
T_1, T_2
2) $r_{s1} \in_R \mathbb{Z}$
r_{s1}
3) $\dot{r}_{s1} \leftarrow x(r_{s1}P)$
$\dot{r}_{s1} \leftarrow x(r_{s1}P)$
4) $T_3 \leftarrow (r_{t1} + \dot{r}_{s1}x_1)Y$,
$T_4 \leftarrow (r_{t2} + \dot{r}_{s1}x_1x_2)Y$
T_3, T_4
5) $(y^{-1}T_3 - T_1)\dot{r}_{s1}^{-1} = x_1P$
(Look up x_1 and X_2 paired with x_1P)
6) If $(y^{-1}T_4 - T_2)x_1^{-1}\dot{r}_{s1}^{-1} = X_2$, then accept else reject.

Fig. 7. ID&Pwd-Transfer Scheme combined (Protocol 2)

Since $(x_1 - x_1x_2)Y$ is a fixed value for a specific tag, it can be used to track a tag. This protocol does hence not provide any privacy protection.

To overcome this problem, one needs to use independent random numbers in the ID-transfer scheme and the Pwd-transfer scheme, as is shown in Fig. 7. Protocol 2 can be considered as two instances of the ID-transfer scheme which are executed in parallel. One protocol instance uses the secret ID x_1, the other one uses the secret ID $x_3 = (x_1x_2)$. Since x_2 is random and independent of the value x_1, and since r_{t1} and r_{t2} are two independent random values, both protocol instances are hence independent. They only use the same challenge r_{s1}. Note that the following two statements hold:

- The ID-transfer scheme can be reduced to the Schnorr protocol (as is demonstrated in Sect. 3.3). The former is hence at least as secure as the latter.

- The Schnorr protocol offers protection against active man-in-the-middle attacks, including the reuse of the same challenge in different protocol instances.

By combining these two findings, one can prove that protocol 2 inherits the security properties of the ID-transfer scheme (protocol 1).

The same argumentation can be used to prove the privacy properties of protocol 2. Both a narrow-strong and a wide-weak attacker can perform man-in-the-middle attacks, where the same challenge is sent to one particular tag in several different protocol instances. Since the ID-transfer scheme is narrow-strong and wide-weak privacy-preserving, the parallel execution of two protocol instances using the same challenge r_{s1} does not change its privacy properties. Protocol 2 is hence also narrow-strong and wide-weak privacy-preserving.

3.6 Hardware Realization

The two secure and privacy-preserving authentication protocols proposed in this paper rely exclusively on the use of Elliptic Curve Cryptography. They do not require other cryptographic building blocks. A hardware architecture that realizes the computation required in our RFID protocols is presented in [17]. The processor is composed of a micro controller, a bus manager and an EC processor (ECP). It has a power consumption of $11.33\mu W$ and it can complete any of the protocols in less than 300 ms. In addition, it can be produced with less than 15 Kgates. These performance results show the feasibility of the protocols proposed even for a passive tag and outperform other secure and private protocols proposed in the literature.

4 Conclusions

In this paper, we have addressed the risk of tracking attacks in RFID networks. We gave an overview of cryptographic authentication protocols which have been proposed so far, and discussed the public-key based techniques more in detail. We proposed two new authentication protocols that are exclusively based on the use of Elliptic Curve Cryptography. Both RFID authentication protocols are narrow-strong and wide-weak privacy preserving. To the best of our knowledge, our protocols are the first ECC-based authentication protocols which offer privacy protection against a wide-weak attacker. Each of the protocols has different computational demands and accordingly different security features. Compared to other RFID schemes proposed in the literature, our protocols remain lightweight in terms of area and computation time, while still achieving the required security and privacy properties.

Acknowledgments

This work was partially supported by the US National Science Foundation CCF-0541472, by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy), by K.U. Leuven-BOF (OT/06/40), by the FWO project G.0300.07, and by the Flemish IBBT projects.

References

1. Avoine, G.: Adversarial Model for Radio Frequency Identification. Cryptology ePrint Archive, Report 2005/049 (2005), `http://eprint.iacr.org/`
2. Bellare, M., Palacio, A.: GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 162–177. Springer, Heidelberg (2002)
3. Berbain, C., Billet, O., Etrog, J., Gilbert, H.: An efficient forward private RFID protocol. In: Proceedings of the 16th ACM conference on Computer and communications security (CCS 2009), pp. 43–53. ACM, New York (2009)
4. Bringer, J., Chabanne, H.: Trusted-HB: A Low-Cost Version of HB^+ Secure Against Man-in-the-Middle Attacks. IEEE Transactions on Information Theory 54(9), 4339–4342 (2008)
5. Bringer, J., Chabanne, H., Dottax, E.: HB^{++}: a Lightweight Authentication Protocol Secure against Some Attacks. In: Security, Privacy and Trust in Pervasive and Ubiquitous Computing - SecPerU (2006)
6. Bringer, J., Chabannel, H., Icart, T.: Cryptanalysis of EC-RAC, a RFID Identification Protocol. In: Franklin, M.K., Hui, L.C.K., Wong, D.S. (eds.) CANS 2008. LNCS, vol. 5339. Springer, Heidelberg (2008)
7. Danev, B., Heydt-Benjamin, T.S., Čapkun, S.: Physical-layer Identification of RFID Devices. In: Proceedings of the 18th USENIX Security Symposium (USENIX Security 2009), pp. 125–136. USENIX (2009)
8. Deursen, T., Radomirović, S.: Attacks on RFID Protocols. In: Cryptology ePrint Archive: listing for 2008 (2008/310) (2008)
9. Deursen, T., Radomirović, S.: Untraceable RFID protocols are not trivially composable: Attacks on the revision of EC-RAC. In: Cryptology ePrint Archive: Report 2009/332 (2009)
10. Fan, J., Hermans, J., Vercauteren, F.: On the Claimed Privacy of EC-RAC III. Cryptology ePrint Archive, Report 2010/132 (2010), `http://eprint.iacr.org/`
11. Feldhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong Authentication for RFID Systems using the AES Algorithm. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 357–370. Springer, Heidelberg (2004)
12. Frumkin, D., Shamir, A.: Un-Trusted-HB: Security Vulnerabilities of Trusted-HB. In: Proceedings of RFIDSec 2009, Leuven, Belgium (2009)
13. Gilbert, H., Robshaw, M., Sibert, H.: An active attack against HB^+ - a provably secure lightweight authentication protocol. IEE processing letters 41(21), 1169–1170 (2005)
14. Hein, D., Wolkerstorfer, J., Felber, N.: ECC is Ready for RFID - A Proof in Silicon. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 401–413. Springer, Heidelberg (2009)
15. Juels, A., Weis, S.: Defining Strong Privacy for RFID. Cryptology ePrint Archive, Report 2006/137 (2006), `http://eprint.iacr.org/`
16. Juels, A., Weis, S.: Authenticating pervasive devices with human protocols. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 293–308. Springer, Heidelberg (2005)
17. Lee, Y.K., Batina, L., Singelée, D., Verbauwhede, I.: Low-Cost Untraceable Authentication Protocols for RFID. In: ACM Conference on Wireless Network Security - WiSec 2010. ACM, New York (2010)
18. Lee, Y.K., Batina, L., Verbauwhede, I.: EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. In: IEEE International Conference on RFID, pp. 97–104. IEEE, Los Alamitos (2008)

19. Lee, Y.K., Batina, L., Verbauwhede, I.: Untraceable RFID Authentication Protocols: Revision of EC-RAC. In: IEEE International Conference on RFID, pp. 178–185. IEEE, Los Alamitos (2009)
20. Lee, Y.K., Sakiyama, K., Batina, L., Verbauwhede, I.: Elliptic Curve Based Security Processor for RFID. IEEE Transactions on Computer 57(11), 1514–1527 (2008)
21. Ng, C., Susilo, W., Mu, Y., Safavi-Naini, R.: RFID Privacy Models Revisited. In: Jajodia, S., Lopez, J. (eds.) ESORICS 2008. LNCS, vol. 5283, pp. 251–266. Springer, Heidelberg (2008)
22. NIST National Institute of Standards and Technology. Cryptographic Hash Algorithm Competition, `http://csrc.nist.gov/groups/ST/hash/sha-3/index.html`
23. Okamoto, T.: Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 31–53. Springer, Heidelberg (1993)
24. Schnorr, C.-P.: Efficient Identification and Signatures for Smart Cards. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 239–252. Springer, Heidelberg (1990)
25. Toiruul, B., Lee, K.: An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems. International Journal of Computer Science and Network Security 6(9B) (September 2006)
26. Tuyls, P., Batina, L.: RFID-tags for Anti-Counterfeiting. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 115–131. Springer, Heidelberg (2006)
27. Vaudenay, S.: On privacy models for RFID. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 68–87. Springer, Heidelberg (2007)

A Preliminary Study of a Wireless Process Control Network Using Emulation Testbeds

Michele Guglielmi, Igor Nai, Andres Perez-Garcia, and Christos Siaterlis

European Commission, Joint Research Centre,
Institute for the Protection and Security of the Citizen
Via E. Fermi 1, 21027 Ispra, VA, Italy
`firstname.surname@jrc.ec.europa.eu`

Abstract. The increasing dependence of Critical Infrastructures (CI) from Information and Communication Technologies might encompass significant risks to our society. Experimentation with CI before introducing a new technology has always been difficult mainly because the architecture complexity, the inability to conduct experiments within a mission critical environment as well as the lack of specialized tools for recreating a CI. In this paper we present the first results of a study that was conducted in a specialized environment for experimenting with CI. We propose the use of an emulation testbed (Emulab driven) along with SCADA-aware components in order to recreate a typical Process Control Network (PCN). We present here experimental results of the risks that operators might face while installing Wi-Fi access technologies within a PCN. This work is indicative of the approach, that operators could follow, to measure, understand and minimize undesirable consequences to the resilience of a CI.

Keywords: Critical Infrastructures, SCADA, emulation, resilience.

1 Introduction

IP network technologies, due to their efficiency and the potential for cost-savings, have been increasingly deployed within many different types of Critical Infrastructures (CI), e.g., in the energy and the gas and oil sectors. Recently, this increasing use and dependence of CI from the Internet and IP data networks in general, has triggered concerns about the security of our CI. These concerns are depicted in many policy initiatives under the theme of Critical Infrastructure Protection (CIP) [6],[9] and have triggered the launch of several research activities for the protection of our CI.

This trend, i.e., the proliferation of IP networks, is expected to continue in the years to come as Critical Next Generation Infrastructures will utilize and depend from -a still undefined- Future Internet. One of the main elements of the Future Internet is in general agreement the massive use of wireless technologies. Activities that have reached the news, already indicate that the use of wireless IP networks within Critical Next Generation Infrastructures, e.g., the SmartGrid,

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 268–279, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

is highly probable [2]. But whenever new technologies and architectures are introduced a systematic study of security and resilience aspects of a CI is deemed mandatory. On the other hand, in contrast with other application environments, experimentation within the production network of a CI is prohibited by the high risk of disruption of mission critical systems. We approach this problem by using emulation testbeds, e.g., like Emulab [1] and DETER [3], in order to abstract CI networks and conduct security related experiments. The use of emulation testbeds as a platform to systematically study Process Control Networks (PCN) and Supervisory Control And Data Acquisition protocols (SCADA) has been mentioned in 2008 by Giani et al. [7] but this effort is still in the first stages of development.

In our paper we present a full scale implementation of an emulation testbed suitable for testing and evaluating of resilience characteristics of a CI network.The testbed is augmented by our Programmable Logic Controller (PLC) simulator, that allows the instantiation of a SCADA speaking PLC in a generic PC, and a SCADA master simulator that communicates with PLCs using the Modbus protocol. The developed components allow any researcher working in this field to easily recreate a typical PCN. Furthermore, we present the first experimental results that display the effects that the introduction of wireless networking can incur in a Modbus/SCADA controlled industrial site. Our results indicate that the use of a wireless network can introduce significant delays with undesirable consequences to SCADA controlled processes even in cases of low network utilization.

The paper is structured as follows. We begin in Section 2 with a presentation of a typical industrial CI network and the challenges that the introduction of new technologies can bring. In Section 3 we describe briefly how we can recreate a CI network architecture using an emulation testbed and we continue in Section 4 with the details of our experiments, that investigate concerns about the resilience of SCADA communications over a IEEE 802.11 Wi-Fi network. Finally in Section 5 we summarize the main conclusions of our study.

2 Industrial ICT Critical Infrastructures

In modern “Industrial Process Control Network Architectures”, one can identify two different control layers: (i) the physical Layer composed of all the actuators, sensors, and generally speaking hardware devices that physically perform the actions on the system (e.g. open a valve, measure the voltage in a cable etc.); (ii)the Cyber-Layer composed of all the ICT devices and softwares which acquire the data, elaborate low level process strategies and deliver the commands to the physical layer. The cyber-layer is typically using SCADA protocols to control and manage the industrial installation. The whole architecture can be thought as a “distributed control system” spread among two networks: the *Control Network* and the *Process Network*. The process network hosts usually all the SCADA servers and HMI(Human Machine Interface). The control network hosts all the devices which, on one side control the actuators and sensors of the physical layer and on the other side provide the “control interface” to the process network.

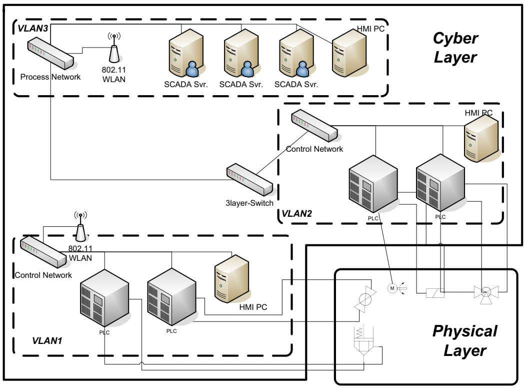


Fig. 1. Example of an Industrial Plant Network

A typical control network is composed by a mesh of *PLC*(Programmable Logic Controller) as shown in Figure 1.

The PLCs receive data from the physical layer, elaborate on the basis of that data a "local actuation strategy", and send back to the actuators commands. The same PLCs provide, when requested, the data received from the physical layer to the SCADA servers (Masters) in the process network, and eventually execute the commands received by them.

In modern SCADA architectures, the communication between Master and PLCs, is usually implemented in two different ways: (i) Through an OPC (Object Linking and Embedding (OLE) for Process Control)layer which help in mapping the PLC devices, (ii) through a direct memory mapping notation making use of the support of some well known SCADA protocol like Modbus (which we will use in this paper as reference since is one of the most used in the field of Industrial Informatics). Modbus is an application layer messaging protocol, positioned at level 7 of the OSI model providing client/server communication between devices connected on different types of buses or networks. The devices can be connected with different networks or buses: EIA-232, EIA-422, kEIA-485 or TCP/IP. A communication transaction comprises a single query and single response frame or a single broadcast frame. Important parameters in a Modbus communication are the **scan rate** with which a Master queries a set of PLCs and the **response timeout**. The exact scan rates depend on the type of installations and processes controlled. The Modbus protocol defines a simple protocol data unit (PDU) independent from the underlying communication layers. Usually, to map Modbus on a specific bus or network, a set of additional fields are added to the application data unit (ADU). The Modbus application data unit is built by the entity that initiates a Modbus transaction (Figure 2). The function code indicates to the slave what kind of action to perform. The data field contains additional information that the PLC uses to take the requested action. The data field may be empty if additional information is not needed. If no errors occur, the requested data are sent back from the PLC to the Master. If an error occurs,

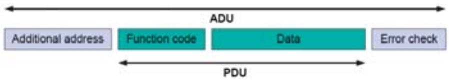


Fig. 2. Illustration of the Modbus ADU

the returning ADU contains an exception code which will be used by the Master to determine the next action to be taken. In average the size of a typical Modbus ADU is 100 Bytes.

3 Recreating a PCN Using an Emulation Testbed

The computing and networking architectures that are typically found within a CI are of significant size and complexity. A typical Process Control Network (PCN) consists of a large number of similar devices (e.g. PLCs), a few standard components (e.g. workstations for HMI) and a small number of specialized servers (SCADA servers/DCS). Using an ad-hoc testbed for experimentation is not recommended because it is very time-consuming and error-prone to setup, maintain and change. An alternative approach is the use of an emulation testbed to recreate the network architecture of a CI. Specifically, our laboratory's testbed is using the Emulab architecture and software [1] which allows us to automatically and dynamically map physical components (e.g. servers, switches) to a virtual topology. In other words the Emulab software configures the physical topology in way that it emulates the virtual topology as transparently as possible [3]. This way we gain significant advantages in terms of repeatability, scalability and high level of realism of our experiments [10].

Our emulation testbed consists mainly of two servers running the Emulab software and a pool of physical resources (e.g. generic PCs and network switches) that are free to be used as experimental nodes. The following steps (Figure 3) describe the re-creation of a PCN network architecture within our testbed:

1. First we need to create a detailed description of the PCN using an extension of the NS language [8];
2. In our description we enumerate similar components as different instances of the same component type (e.g a Virtual-PLC). This way pre-defined templates of different components can be easily reused and automatically deployed and configured.
3. Whenever we want to run an experiment we instantiate it by using the Emulab software. The Emulab server automatically reserves and allocates the physical resources that are needed from the pool of available components;
4. Furthermore the software configures network switches in order to recreate the virtual topology by connecting experimental nodes using multiple VLANs;
5. Finally before the testbed is released for experimentation the software configures packet capturing of predefined links for monitoring purposes.

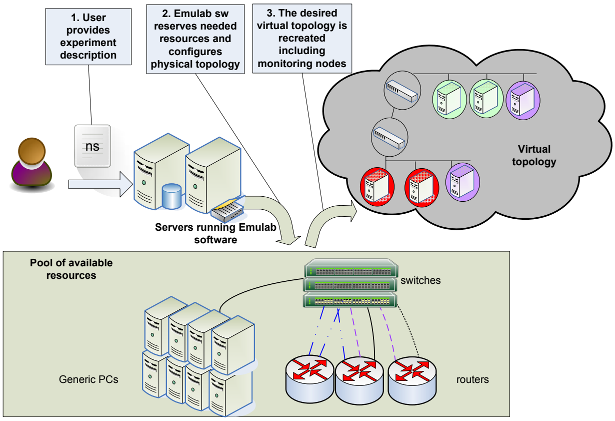

1. User provides experiment description
2. Emulab sw reserves needed resources and configures physical topology
3. The desired virtual topology is recreated including monitoring nodes
ns
Virtual topology
Servers running Emulab software
Pool of available resources
switches
Generic PCs
routers

Fig. 3. Main steps for recreating a PCN network within an Emulab-based testbed

As we mentioned in step 2, we have developed templates for typical PCN components. These are practically disk images that can be transparently loaded and run on top of generic PCs. Their main elements are: an Operating System (Windows) and the simulation software that corresponds to the specific component type. In our case we have developed:

- a Virtual-PLC, that simulates a Modbus speaking PLC able to a) Read Coils b) Write Coils etc.
- a Virtual-SCADA-Master that simulates the behavior of a SCADA server that periodically collects information from PLCs using the Modbus protocol, with configurable scan rate and response timeout, and acts based on the collected information.

These components could allow any researcher working in this field to easily recreate a typical PCN and we intend to publish them on the web as soon as we port them into a free OS, e.g., Linux.

4 Introduction oOf Wi-Fi in a PCN, a Case Study

The evolution of telecommunication technologies has also changed Industrial networks. First, there was a migration from the traditional RS-485 communication channel to IP based networks. Today we see that the use of IP wireless networks for industrial systems has been proposed. Of course, classic IEEE 802.11 systems can be only used by devices having direct access to a power source, since the Wi-Fi technology is power consuming. This fact, was the starting point for the development of new standards, such as 6LoWPAN, the IETF draft standard for IPv6 over 802.15.4 that provides a wireless connection service with low power consumption, at the price of lower transmission power. The IEEE 802.15.4 protocol [4] is already used today by ZigBee [5] and WirelessHart [11]. The advantages of the introduction of wireless technologies in critical industrial infrastructures are evident: less cables within the installation, more flexibility etc. However, the use of wireless communications and especially technologies with low-power transmission, in industrial settings poses serious questions about their reliability, robustness and resilience. One of the concerns is the effect of "interferences", because an industrial CI is a place that is exposed, per se, to electromagnetic interferences, for example generated by electro-mechanical devices like gas turbines. The need for systematic studies on the drawbacks deriving from the use of wireless communications into critical industrial infrastructures is high. However, due to the highly complex interactions between the different elements of a process system, every theoretical and "off-line" analysis, in order to be considered consistent, has to be supported by field tests. These tests, considering the criticality of the process system of a power plant, could be hardly performed safely into a real, in production, installation. An architecture such as the one presented in the previous sections could be extremely useful for process engineers, to quickly re-create industrial environments and study how a process system would react, to interferences and attacks. The approach could be used to answer questions like:

1. How could the use of Wi-Fi within a PCN affect the process reaction delay under different traffic loads ?
2. Which is the maximum bandwidth that a process network can sustain without performance degradation, given parameters like Master scan rate, PLC response timeout etc. ?
3. How many PLCs can an access point handle under different traffic loads?
4. Is there a difference in this number if the process system is in a different state?
5. Is a Wi-Fi network equivalent to the wired network, or are there constraints particular to specific process systems that might discourage the use of Wi-Fi?

To show the potential of our approach, we describe in the next section how we have tried to provide an answer to the first question for a well defined, even if simplified, process system, composed by Virtual PLCs controlling valves and temperature sensors, and a typical SCADA Master.

4.1 Experimental Setup

With the use of our Emulab testbed, we have recreated an experimental environment consisting of a SCADA Master, a wireless PLC, a wired PLC, a traffic generator and a traffic sink. The wireless network is composed of a "commercial, off-the-shelf" (COTS) access point and all components are connected to the same IP subnet (10.1.1.0/24) as shown in Figure 4 and described in the table 1 that follows. All nodes have either wireshark or tcpdump for monitoring and troubleshooting purposes. Iperf is used both in the traffic generator and the sink node to inject background traffic (bidirectional 200 byte UDP packet streams)

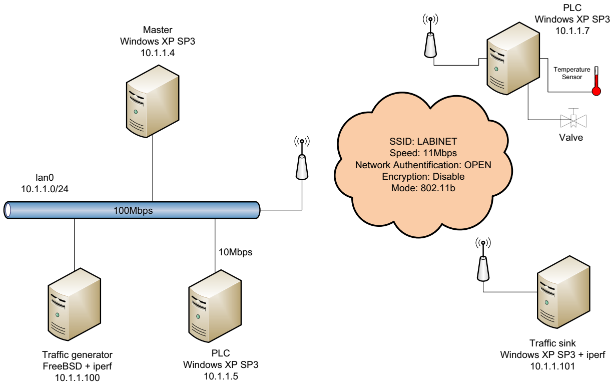


Fig. 4. Topology of the PCN that is used in our experiments

Table 1. Description of experimental nodes

	Master	Wireless PLC	Traffic generator	Traffic sink
Hardware	PC Dell	PC Dell	PC Dell	PC Dell
Interface	Intel Pro 10/100/1000	USB Wireless	Intel Pro 10/100/1000	USB Wireless
Operating System	Win. XP SP3	Win. XP SP3	FreeBSD 6.3	Win. XP SP3
Additional software	Virtual-SCADA-Master	Virtual-PLC	Iperf	Iperf

within the wireless network. This background traffic is intended to simulate traffic from other wireless PLCs associated to the same access point. Therefore, it allows us to test the system's behavior under different load conditions. Emulab inserts transparent nodes in order to model the network in terms of delay, packet loss and bandwidth. Initially, we define a LAN with neither delay nor packet loss, and a bandwidth of 100Mbps. During the experiments, we are able to change these parameters through dynamic events. The wireless network is configured with a bandwidth of 11Mbps, Open authentication and no encryption. Using this topology, we have performed two sets of experiments:

1. Application delay and packet discard rate vs. background traffic. Discarded packets are the packets that either arrive at the application level after the expiration of the response timeout (e.g., 20 ms) or are dropped in the network. In this experiment, the Master sends 1000 queries to the PLC with a scan rate of 60ms and measures the delay of the responses. This scenario intends to simulate a near to real time process, where delay in the response above 20ms is considered high. At the beginning we start without background traffic and we increase it gradually.
2. Application delay vs. packet discard rate. Here, packet discard rate is the only parameter we change through dynamic events in order to test the application delay. The PLC measures a variable that changes with time. The Master has to be able to accurately capture this variation in order to act, e.g., to open a safety valve when the temperature rises above a certain threshold.

As the discard rate increases, the Master will be aware of the variation with a potentially critical delay.

Eventually, we can correlate both experiments to infer how much traffic an access point is able to handle without provoking degradation at the application level.

4.2 Experimental Results

In the first experiment we study the influence of background traffic to the application delay and to the packet discard rate. In the case of a wired network this effect is minimal due to the high performance of the network components. In the wireless network all devices are connected to the same access point and share the collision domain, limiting the network performance. Furthermore it is worth to point out that we have installed the access point and the wireless nodes inside the lab, where we have an infrastructure consisting of switches, servers, PCs, monitors, cooling systems etc. All them are source of electromagnetic interferences which also affects the wireless network performance and stability. We expect that the interferences could be even more severe in an industrial environment such as an electricity power plant.

Figure 5(a) shows the percentage of packets that either arrive out of time at the application level (20 ms) or get dropped in the network (discarded packets), versus the background traffic for both a IEEE 802.11b PLC and a wired 10BASE-T PLC. In Figure 5(b) we show the change of the average delay at the application level. With the wired PLC the network is able to handle nearly 7Mbps of bidirectional traffic without affecting the application, whereas in the wireless experiment we reach some conclusions:

1. There is a variation in the performance of the wireless network therefor we have added a trend line to make the analysis easier.
2. The amount of background traffic the network is able to handle is limited to less than 2Mbps if we require a delay lower than 20ms and a packet discard rate below 1%.

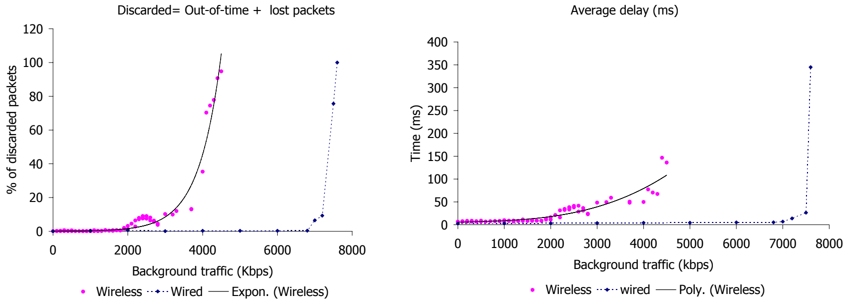


Fig. 5. (a) Experienced packet discards with varying background traffic (wireless). (b) Experienced delay with varying background traffic (wireless).

3. These results could significantly change depending on the hardware due to the use of relatively small packets as background traffic. Since we have used a COTS access point, its performance is limited in terms of packet switching.

Our experiment shows how the introduction of wireless connections in industrial systems, can cause a non negligible effect in terms of delay and packet discard rate, even under moderate traffic load. Therefore an in-depth study of the number of PLCs that will be connected to the wireless network has to be undertaken in order to guarantee the stability of the application performance. The following experiment demonstrates the impact of increasing packet discard rate on the reaction time of a process control application.

In the second experiment, a PLC is connected to a temperature sensor and the Master monitors the temperature by querying the slave every n-milliseconds, where n is the "scan rate". We use "scan rates" of 60 and 120 milliseconds. When the temperature reaches a certain level, the Master sends a command to open a safety valve. The temperature sensor in our platform is simulated by our Virtual-PLC and the temperature increases each 1 millisecond, following a quadratic curve. For presentation purposes, in the figures that follow we focus on a small portion of the whole curve. In Figure 6 the thick line represents the temperature of the sensor which changes every millisecond, the dashed line represents the temperature read by the master with a scan rate of 60 ms and the thin line the temperature read by the master with a scan rate of 120 ms. For example if we assume that the master should trigger an action when the temperature exceeds 24.1 degrees:

- The real temperature of the sensor exceeds 24.12 degrees at time 4,9113.
- The master with 60 ms scan rate notices it at time 4,9171 (58 ms later).
- The master with 120 ms scan rate notices it at time 4,9203 (90 ms later).

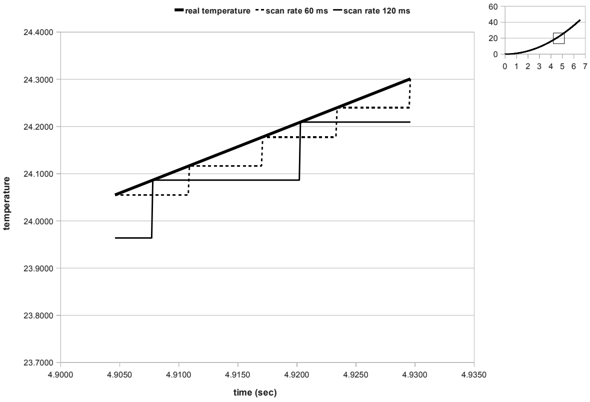
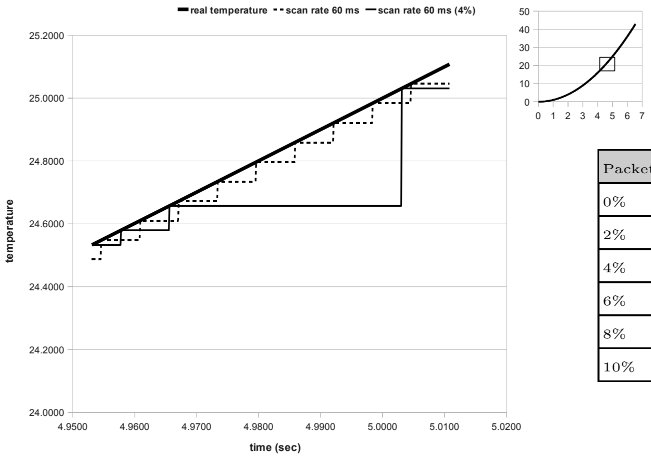


Fig. 6. The temperature perceived by the master with scan rate of 60 and 120 ms



Packet Discards (%)	Average Delay
0%	68.53
2%	107.62
4%	213.11
6%	363.38
8%	618.31
10%	983,5

Fig. 7. The temperature perceived by the master under different packet discard rates

These kind of tests are very useful for designers of CI. The choice of scan rate in the master can significantly influence the control of remote devices in real-time processes. Here, we will illustrate the magnitude of the delay that a monitoring process might experience under different packet discard rates. Using our emulation testbed, we conduct an experiment where the master reads the temperature from the PLC every 60 ms, under different packet discard rates: 0%, 2%, 4%, 6%, 8%, 10%; Figure 7 shows the average delays that the master experiences while getting the temperature from the PLC. If we consider for example the first line of the table in Figure 7 and that the temperature grows every 1 ms, then the master with a scan rate of 60 ms will lose 60 values between a request and the next one. The value in the first row is 68, because the scan rate is 60 ms, but considering the time to send the request to the slave and the time to read the value from the register, then 68 is the number of actual temperature values lost by the master. The average delay will eventually increase once the packet discard rate gets higher. In more details, the thick line represents the real temperature, the dashed line represents the temperature read by the master with a scan rate of 60 ms (0% packet loss) and the thin line the temperature read by the master with a scan rate of 60 ms and a packet discard rate of 6%. The thin line follows the same trend as the dashed line except for a big jump between time 4.9656 and time 5.0030 (374 ms). This jump represents a lost packet and has a great impact on performance, because in the case of the dashed line the master has lost 6 values more than in the case of the thin line.

Let us now discuss the potential consequences. The Master should monitor the temperature sensor, and if the temperature become higher than a certain value, it should immediately open a safety valve. In normal conditions, without packet discards, we would expect a delay in taking the “emergency action” of 68 ms. Considering instead the case of 10% packet losses, the delay would be near to 1 sec., a delay that be critical. Coming back to the results of the first experiment, it is obvious that wireless connections are more vulnerable to such events than wired connections. Moreover, it is evident how industrial protocols like Modbus, that require low time-out and fast scanning rates, might pay a high cost for been ported on top of TCP rather then on UDP. Even if some "implementations" of Modbus over UDP exist, traditionally the industrial community encourage their use only in very limited and specific cases. Unfortunately typical control processes assume near-to-real-time responses, imposing significant constraints on the performance of TCP industrial protocols. But with the use of a platform like the one we have presented, the effects of the introduction of new technologies such as a Wi-Fi network could be studied using an empirical approach.

5 Conclusions and Future Work

In this paper we have demonstrated how emulation testbeds (e.g. based on Emulab) can be used to study the resilience characteristics of Process Control Networks that lie in heart of many Critical Infrastructures. The motivation is threefold: a) experimentation on top of production infrastructures is impossible; b) it is cumbersome and inefficient to recreate CI network architectures with ad-hoc testbeds due to their scale and complexity; c) the use of advanced emulation testbeds can offer significant advantages in terms of experiment repeatability and thus reliability of the results.

Furthermore, we present a preliminary study of the effects that the introduction of wireless networking technologies (such as Wi-Fi) can have on the SCADA communications within an industrial network. Our results show that the use of a wireless network can introduce significant delays in comparison to a wired network with undesirable consequences to SCADA controlled processes even in cases of low network utilization. Our results could help process engineers make informed decisions about the use of Wi-Fi technologies to support SCADA communications.

Our work may be extended in the future towards multiple directions:

1. Assess the impact of other parameters that influence real SCADA applications (e.g., packet re-ordering);
2. Assess the impact of parameters related to the wireless technology (e.g., background noise and interferences, use of other technologies like GPRS, Tetra, WiMax, IEEE 802.15.4);
3. Assess the impact of cyber-attacks (e.g. Denial of Service attacks, Ad-hoc Malware attacks);
4. Assess the impact of lightweight encryption technologies (ID Based Signatures, Elliptic Curves etc.) on the performances of SCADA applications;
5. Connect the emulation testbed with a simulator of physical processes (e.g. generators and turbines) in order to study how events happening in cyberspace can affect physical systems.

References

1. Emulab, http://www.emulab.net/
2. Alvarion. Alvarion and National Grid conduct smart power grid proof of concept in the U.S. Press release (2009)
3. Benzel, T., Braden, R., Kim, D., Neuman, C., Joseph, A.D., Sklower, K.: Experience with DETER: A testbed for security research. In: TRIDENTCOM (2006)
4. De Nardis, L., Di Benedetto, M.-G.: Overview of the IEEE 802.15.4/4a standards for low data rate wireless personal data networks. In: 4th Workshop on Positioning, Navigation and Communication, pp. 285–289 (2007)
5. Egan, D.: The emergence of Zigbee in building automation and industrial control. Computing & Control Engineering Journal 16(2), 14–19 (2005)
6. European Commission: Communication on CIIP - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM, 149 (2009)
7. Giani, A., Karsai, G., Roosta, T., Shah, A., Sinopoli, B., Wiley, J.: A testbed for secure and robust SCADA systems. SIGBED Rev. 5(2), 1–4 (2008)
8. ISI. Network simulator NS-2, http://www.isi.edu/nsnam/ns/
9. U.S. Department of Homeland Security (DHS). Protecting infrastructure: Critical infrastructure and key resources (cikr), http://www.dhs.gov/files/programs/gc_1189168948944.shtm
10. Siaterlis, C., Masera, M.: A review of available software for the creation of testbeds for internet security research. In: 1st International Conference on Advances in System Simulation, pp. 79–87 (2009)
11. Song, J., Han, S., Mok, A.K., Chen, D., Lucas, M., Nixon, M.: Wirelesshart: Applying wireless technology in real-time industrial process control. In: IEEE Real-Time and Embedded Technology and Applications Symposium, pp. 377–386 (2008)

CogProt: A Framework for Cognitive Configuration and Optimization of Communication Protocols

Dzmitry Kliazovich[1], Neumar Malheiros[2], Nelson L.S. da Fonseca[2],
Fabrizio Granelli[1], and Edmundo Madeira[2]

[1] DISI – University of Trento
Via Sommarive 14, I-38050 Trento, Italy
{kliazovich,granelli}@disi.unitn.it
[2] Institute of Computing – University of Campinas
Av. A. Einstein, 1251, 13083-970 Campinas, Brazil
{ncm,nfonseca,edmundo}@ic.unicamp.br

Abstract. Advancements in network technologies dramatically increased management complexity. Cognitive networking was introduced to deal with this problem, by providing algorithms for autonomous network management and protocol reconfiguration. In this paper, we propose a framework for cognitive configuration and optimization of communication protocols called CogProt. CogProt is a distributed framework that allows dynamic reconfiguration of operational protocol stack parameters for optimizing protocol performance under changing network conditions. As a proof of concept, the framework is illustrated for the cognitive configuration of TCP congestion window evolution. In this setup, the TCP window increase factor is adjusted in runtime based on the TCP goodput experienced in the immediate past. Simulation results demonstrate that the proposed cognitive framework is able to improve average TCP performance under changing network conditions.[1]

Keywords: cognitive networks, self-configuration, cognitive TCP.

1 Introduction

Degradation of performance due to time-varying network conditions is a challenging issue that needs to be properly addressed by current network research. The dynamic adjustment of the protocol stack parameters in a cognitive fashion is a promising approach to deal with that issue. Such idea was introduced by Mitola [6], along with the concept of cognitive radio to provide efficient spectrum sharing by avoiding interference among communication systems.

Actually, cognitive radio is limited to the ability to tune the parameters of physical and link layers while following local optimization goals. On the other

---

[1] This work is supported by the Italian Ministry in the framework of WORLD (Wireless multiplatfOrm mimo active access netwoRks for QoS-demanding muLtimedia Delivery) project and by FAPESP under grant number 2006/50512-4.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 280–291, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

hand, the broader concept of cognitive networks [8,3] considers system-wide goals and cross-layer design[7,9]. Cognitive network is a recently emerged networking paradigm that combines cognitive algorithms, cooperative networking, and cross-layer design in order to provide real-time optimization of complex communication systems.

The main contribution of this paper is a framework for cognitive configuration and optimization of communication protocols called CogProt. CogProt involves main concepts of the cognitive network approach, such as global vision and optimization of end-to-end goals. It is suitable for joint optimization of multiple protocol layers for different network nodes in a distributed way. CogProt is not only concerned with initial setup of protocol parameters, but also with their runtime reconfiguration and optimization.

The CogProt framework is not limited to finding optimal values for each protocol parameter, but it aims the optimization of network performance by periodically reconfiguring each protocol parameter based on recent (even immediate) experience. Each network node is allowed to decide on the best protocol configuration to fit current network conditions. This way, the CogProt framework is not only able to avoid performance degradation due to time-varying conditions, but also to maximize overall performance for different network scenarios.

In this work, CogProt is applied to the TCP/IP stack as an illustration of its use. Despite its success, the TCP/IP Internet protocol suite still presents fundamental design challenges since its strict design is not able to guarantee the required performance[4,1]. The TCP/IP protocol suite, historically designed for wired networks, neither includes adaptation techniques for heterogeneous and dynamic network environments nor allows communication between layers, which leads to severe limitations in terms of performance. As a proof of concept, we have implemented the CogProt framework into the Network Simulator (ns-2) in order to provide cognitive configuration and optimization of TCP congestion window evolution. Simulation results show performance improvement on TCP average throughput, which demonstrates the feasibility and efficiency of the proposed approach.

Section 2 presents a motivation example, while Section 3 describes the proposed framework. Section 4 discusses on tunable parameters at different protocol stack layers. Section 5 presents performance evaluation of the proposed approach. We describe the simulation scenario and present results considering dynamic adaptation of TCP congestion window increase factor. Finally, Section 6 presents some conclusions and future directions.

2 Motivating Example

The configuration of communication protocols defines the overall performance of applications and data transfer services. However, it is not always possible to anticipate the best setup due to the unpredictable state of the network. For example, the choice for the default initial value of TCP congestion window (w) changed over the time. The original TCP specification defined the initial w value equal to 1 segment. Later, due to a bug in NetBSD implementation, the initial w value was increased to 2 segments. Then, the specification was adapted to allow the initial w value as either 1 or 2 segments. The most recent specification from 2002 [2] permits upper bound for initial w of roughly 4K, which is equivalent to 3 TCP segments. Actually, the authors in [2] proposed setting the initial w value as large as 4 segments in order to improve TCP startup performance.

Advantages of large initial window values include better performance (with TCP receiver implementing Delayed-ACK option) and low protocol delay for tiny-flow applications such as SMTP- and HTTP-based. In addition, large w values enable fast retransmit and fast recovery algorithms right from the beginning of the TCP flow. However, disadvantages of large w values are present in highly congested environments. Although even in such environments, individual flow throughput reduction is rarely observed. The main danger comes from the possibility of congestion collapse of entire network.

In summary, large w values bring performance increase and are desirable in high bandwidth-delay network with low or moderate congestion levels, and should be avoided otherwise. However, there is no way for a network node to know in advance the available network bandwidth and the level of congestion at the end-to-end path between the sender and receiver. Therefore, it is not possible to define the best default value for the initial window. A cognitive approach would dynamically adjust the initial window value for TCP flows according to current network conditions. In Section 4, this problem will be revisited to underline the benefits of the cognitive approach.

3 CogProt Framework

The proposed cognitive framework, CogProt, aims at supporting dynamic configuration and optimization of communication protocols. It provides a way for network elements to adapt their configuration and protocol stack parameters in order to fit constantly changing network conditions. The process of search for optimal setup of protocol parameters is performed by using cognitive algorithms and by sharing information among network nodes. The proposed approach considers the network node architecture presented in Fig. 1. It introduces a cognitive plane in parallel to the protocol layers. This plane is capable of monitoring protocol stack parameters as well as controlling them by issuing configuration commands.

The cognitive optimization process involves a quality feedback loop. For the duration of the optimization process, the cognitive plane monitors the performance of current protocol parameters setup according to well defined target quality metrics. For example, the quality metric for a physical layer parameter could be the measured data rate, while at the application layer the quality metric could be the end-to-end delay for real-time multimedia applications.

The feedback loop iteration is completed with the enforcement of reconfiguration actions from the cognitive plane. These reconfiguration actions are the result of decision-making procedures performed by the cognitive framework. According to the scope they operate, such decision-making procedures can be classified

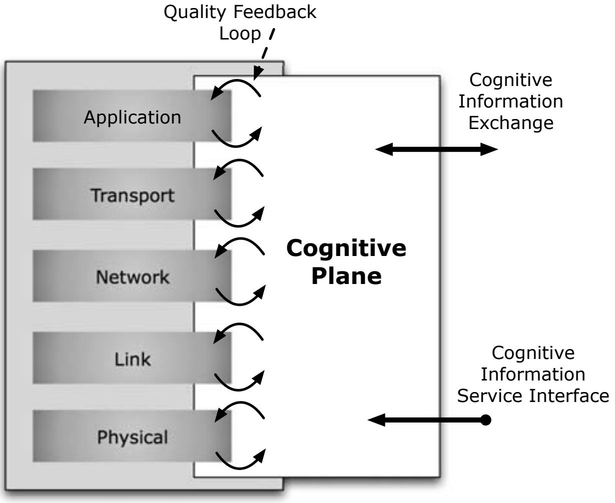


Fig. 1. Cognitive node architecture

into: i) local, which form their decisions based only on locally available information, ii) distributed, receiving additional information from neighboring network nodes, or iii) service-based, requiring reconfiguration policies from a Cognitive Information Service (CIS) fostering cognitive signaling in the local network.

The main task of the cognitive plane is the adaptation of different protocol stack parameters in order to converge to an optimal operational point given the network state. The proposed framework adopts conservative cognitive adaptation to minimize the changes in the protocol stack operation and yet promote convergence to the desired operational point. In the proposed approach, each protocol parameter P is expressed in terms of its default value P_{def} and its operation range $[P_{min}, P_{max}]$. The operation of the protocol is initiated with parameter P set to its default value. Then, the cognitive mechanism begins searching for optimal P values. Such adaptation process is divided in three phases: data analysis, decision-making, and action, as illustrated in Fig. 2.

At the end of an interval I, the cognitive mechanism measures and stores the obtained performance from the current value of P in accordance with the defined quality metric. This *data analysis* phase allows the algorithm to build a knowledge base of performance information on the available values for P along protocol operation. Then, in the *decision-making* phase, the mechanism selects the value of P that provides the best performance according to the performance information base. That value is assigned to the mean of a random number generator that follows a normal distribution. Finally, in the *action* phase, a new value for P is chosen in the range $[P_{min}, P_{max}]$ from the random number generator.

The initial mean for the number generator is P_{def}. This loop continuously adjusts the mean of the normal distribution to the value of P that provides the best performance under current network conditions. Thus, the mean converges

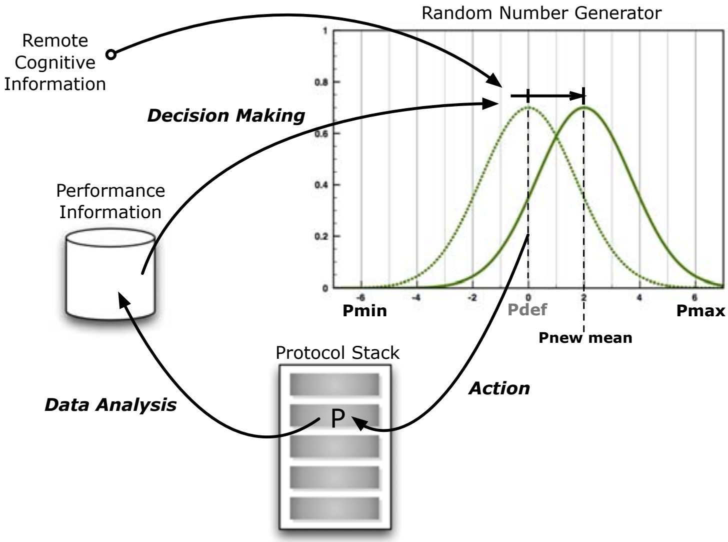


Fig. 2. The quality feedback loop of the cognitive adaptation mechanism

to the optimal value for P. As a result, that optimal value is chosen with a higher frequency since it is the mean of the normal distribution. Meanwhile, the mechanism will choose values nearby the mean, which allow it to react to changes on the network state. The standard deviation assigned to the normal distribution affects the aggressiveness of the mechanism in trying new values of P at each interval I.

CogProt builds a history of operation with different settings and can reconfigure the parameter or adjust future setups based on its past experience. In order to illustrate the operation of the cognitive framework, let us discuss again the problem of setting the initial value of the TCP window size (w) as mentioned in Section 2. The state of end-to-end paths cannot be known "a priori". Therefore, there is a need to properly adjust the initial window to avoid performance degradation. The proposed cognitive mechanism solves that problem by using the described quality feedback loop to constantly trying different values for w in a "smart" way, while monitoring the corresponding protocol performance metrics. CogProt sets most of the flows initiated by the node to use the default value for w, since the default value is the initial mean of the normal distribution. However, from time to time it will use values nearby the mean and update the performance information base. Then, CogProt adjusts the mean of the normal distribution to follow optimal performance.

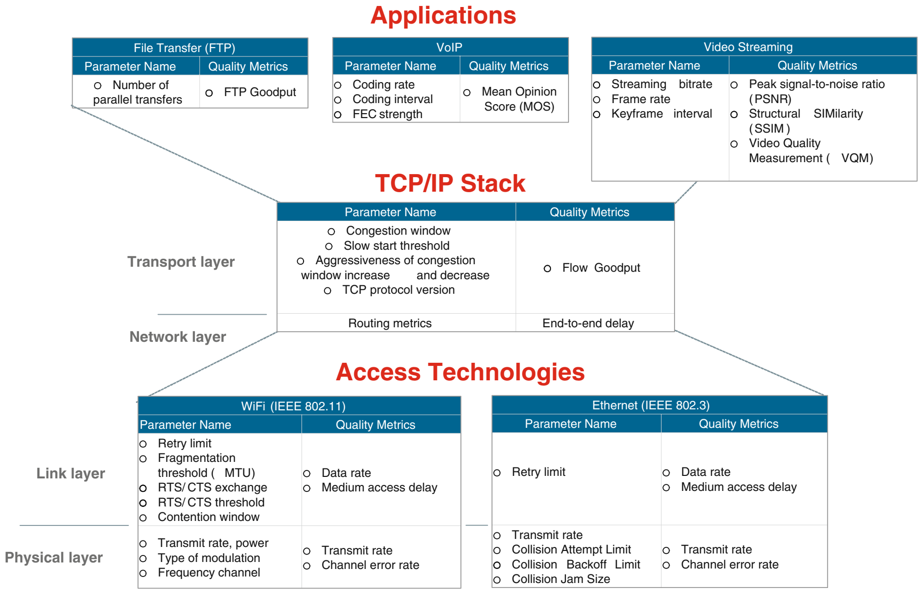
According to proposed approach, the default setup (P_{def}) of the initial window size for TCP flows may be chosen equal to 4K bytes, P_{min} may correspond to 1

MSS (Maximum Segment Size of TCP), while P_{max} may be chosen to be equal to 10 MSSs. This way, by using the proposed cognitive adaptation algorithm, most of the outgoing flows will start with congestion window of 4K, which should deliver optimal performance in normal network conditions. In case of unfavorable conditions, like network congestion, a lower value for w will provide the best performance. On the other hand, in case of unloaded high bandwidth-delay links, a higher value for w will provide the best performance. In both cases, as soon as the algorithm finds the "new" optimal value in the performance table, the mean of the normal distribution is adjusted accordingly. In this way, the mean is dynamically adjusted in order to optimize the protocol performance.

4 Cognitive Tuning of TCP/IP Parameters

The TCP/IP protocol reference model is the de-facto standard for communication on the Internet. It contains a large variety of protocols whose parameters need to be properly configured. Such need has motivated the definition of some protocol variants, for example TCP variants for specific network scenarios. Figure 3 presents a snapshot of the most widely used protocols in the TCP/IP reference model outlining their main configuration parameters and corresponding performance metrics.

The Application layer provides the environment for running user applications. Configurable parameters and quality metrics at this layer depend on the nature of applications. For File Transfer (FTP) applications, a configurable parameter



File Transfer (FTP)

Parameter Name	Quality Metrics
Number of parallel transfers	FTP Goodput

VoIP

Parameter Name	Quality Metrics
Coding rate Coding interval FEC strength	Mean Opinion Score (MOS)

Video Streaming

Parameter Name	Quality Metrics
Streaming bitrate Frame rate Keyframe interval	Peak signal-to-noise ratio (PSNR) Structural SIMilarity (SSIM) Video Quality Measurement (VQM)

TCP/IP Stack

	Parameter Name	Quality Metrics
Transport layer	Congestion window Slow start threshold Aggressiveness of congestion window increase and decrease TCP protocol version	Flow Goodput
Network layer	Routing metrics	End-to-end delay

WiFi (IEEE 802.11)

	Parameter Name	Quality Metrics
Link layer	Retry limit Fragmentation threshold (MTU) RTS/CTS exchange RTS/CTS threshold Contention window	Data rate Medium access delay
Physical layer	Transmit rate, power Type of modulation Frequency channel	Transmit rate Channel error rate

Ethernet (IEEE 802.3)

	Parameter Name	Quality Metrics
Link layer	Retry limit	Data rate Medium access delay
Physical layer	Transmit rate Collision Attempt Limit Collision Backoff Limit Collision Jam Size	Transmit rate Channel error rate

Fig. 3. Tunable TCP/IP Protocol Stack Parameters

could be the number of parallel connections and the main quality metric is the file transfer goodput. For Voice over IP (VoIP) applications, controlling coding rate, coding interval, and Forward Error Correction (FEC) strength helps to increase the voice quality commonly expressed using the Mean Opinion Score (MOS) metric [5].

For video streaming applications, streaming bitrate, framerate, and keyframe interval determine the quality of video flow perception. High bitrates allow video transmissions with high resolutions, high frame rates improve perception of video samples involving high motions, while shorter keyframe intervals improve decoding capabilities in the presence of frame losses or transmission errors.

The Transport layer is generally represented by Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocols. While UDP is mostly passive with the main task of providing differentiation of IP datagrams between different port numbers, TCP implements complex mechanisms including reliable transmissions and flow control. The TCP congestion window evolution is the key factor affecting the flow throughput. Controlling the congestion window increase factor (α) and decrease factor (β) parameters allows improving the flow performance by adjusting the tradeoff between network utilization, protocol fairness, and the level of network congestion.

The Network layer is responsible for routing packets across interconnected networks. Hence, the main performance metric can correspond to the quality of the selected route, for instance in terms of the number of hops or end-to-end delay.

The Link layer serves network layer requests and controls physical layer for different access technologies. Most of the controllable parameters in this layer are determined by the communication technology in use. In Career Sense Multiple Access (CSMA) protocols, such as WiFi IEEE 802.11 or Ethernet IEEE 802.3, the main tunable parameters correspond to the size and evolution of the contention window, as well as the retry limit, which corresponds to the maximum number of retransmission attempts taken at the link layer before a frame is discarded.

The Physical layer parameters are defined by the used network access technology. Wireless access technologies can provide control over the power level of the transmitted signal, choice of the type of modulation, and frequency channel. Fixed network technologies like Ethernet are usually described by collision detection capabilities. Physical layer performance can be defined in terms of the data rate achievable at the physical layer, as well as Bit Error Rate (BER) achieved for the transmitted bit stream.

Indeed, a lot of parameters in the TCP/IP stack need proper tuning. Some of them have a great influence on applications performance. For instance, the parameters governing the TCP transmission window and the initial value of the window have great influence on the performance, especially in networks with high bandwidth delay product.

5 Performance Evaluation

In order to present performance benefits of the proposed approach, we extended the Network Simulator (ns-2) with the required CogProt functionalities to provide dynamic reconfiguration of the TCP congestion window. In particular, the parameter of interest in this evaluation is the TCP congestion window increase factor (α), which controls the evolution of TCP window and, thus, its throughput performance.

5.1 Scenario Description

The simulated topology is illustrated in Fig. 4. It consists of a single source node S and two destination nodes D_1 and D_2 connected using two routers R_1 and R_2. These routers form a bottleneck link of 2 Mbps with the propagation delay of 1 ms. The CogProt framework is implemented only at the source S, while destination nodes and network routers left unmodified.

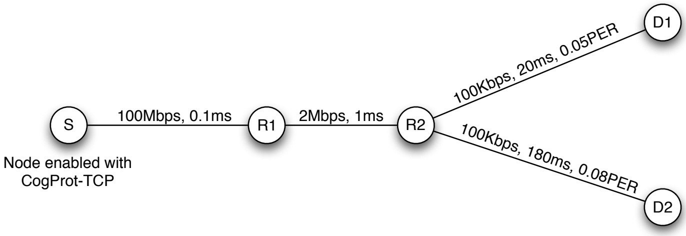


Fig. 4. Simulated topology

Such simulation topology allows establishment of TCP connections that require different window increase strategies depending on the error rate and delay of the last mile link connecting the corresponding destination node. The TCP connection $S - D_1$ has smaller Packet Error Rate (PER) of 5% and delay of 20 ms, while the connection $S - D_2$ experiences higher PER of 8% and larger delay of 180 ms.

Different values of link PERs and propagation delays will require from the flows different window increase strategies in order to obtain optimal performance. High values of α are expected to bring better throughput for high PERs. However, in case of no errors, high values of α will lead to multiple congestion-related losses and throughput degradation due to multiple retransmissions.

In our simulations, we compared the performance of standard TCP NewReno protocol using fixed values for the parameter α with the dynamic reconfiguration of α performed by the CogProt approach.

Average TCP flow throughput is chosen as the main quality metric for the feedback loop. In our simulations, CogProt was allowed to vary the value of the parameter α in the interval $[1, 5]$. A new value for α is selected at the beginning of an interval I equal to 1 second with the standard deviation for the normal distribution (of the random generator) configured at 0.5. The average performance is computed by using an exponentially weighted moving average as follows:

$$T_a = T_a * (1 - s) + T_m * (s) \tag{1}$$

where s is the weight assigned to the immediate throughput (T_m) measured for the current value of α and T_a is the average throughput for the current value of α. The weight of 0.5 was found to provide good tradeoff between the significance of past and present values affecting the speed of algorithms convergence.

5.2 Simulation Results

The CogProt performance was evaluated in three different experiments involving the following TCP flows: $S - D_1$, $S - D_2$, and both $S - D_1$ and $S - D_2$. In the latter case, with two flows, the flow $S - D_1$ was active the first half of the simulation time, while the flow $S - D_2$ during the second half. For all scenarios, the simulation time was 1000 seconds, and the results were the average from 10 runs with a 95% confidence interval.

Fig. 5 shows the average TCP flow throughput for the three experiments with fixed values of α compared with the proposed cognitive mechanism CogProt. For the flow $S - D_1$, experiencing shorter RTT and low error rate, lower values of parameter α lead to optimal performance, while in the other case with flow $S - D_2$ experiencing high error rate and larger RTT, high values of α become desirable. This confirms our assumption that, for any fixed value of α assigned, the flow is going to suffer from performance degradation under specific conditions. However, when CogProt is active (right set of bars in Fig. 5), it is able to keep performance close to optimal for the scenarios with individual flows and outperforms any fixed values of α in the combined scenario. This confirms the benefit of CogProt dynamic adaptation capabilities enabling it to avoid performance degradation in varying network conditions.

Fig. 6 presents the average throughput over time for the experiment with two TCP flows: $S - D_1$ active in the first half of the simulation, and $S - D_2$ active in the second half. The parameter α fixed at 1 performs well for the flow $S - D_1$ and not for $S - D_2$. On the other hand, parameter α fixed at 5 performs well for $S - D_2$ but not for $S - D_1$. This way, performance degradation cannot be avoided by using any fixed value of α. With CogProt the measured TCP throughput corresponds to the best average performance.

In this scenario with both flows, during the first half of the simulation CogProt selected the value of 1 for the parameter α with higher frequency than any other value, while in the second half the value selected with higher frequency is 5. Fig. 7 shows the frequency of selection of different values for α by the proposed algorithm. We can see that the frequency of the value 1 was higher for the flow $S - D_1$ than $S - D_2$, as well as the frequency of the value 5 was higher for the flow $S - D_2$ rather than $S - D_1$.

Results demonstrate the ability of the proposed mechanism to adapt the parameter of interest with a fine granularity. Even considering very short intervals

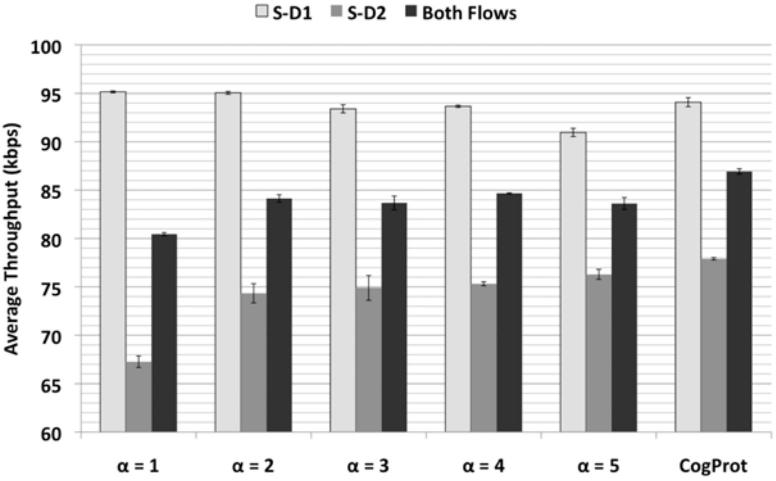


Fig. 5. Average TCP Flow Throughput

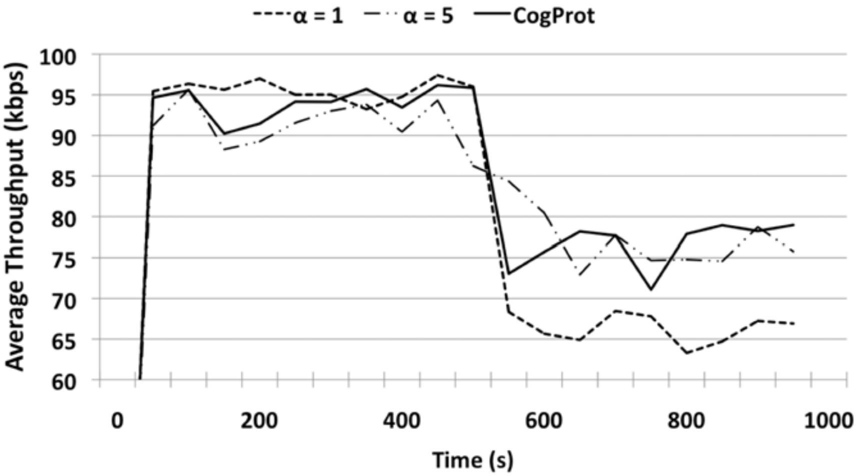


Fig. 6. Average throughput over time in Scenario 3

of reconfiguration (in the order of milliseconds), the mechanism is capable to react to changing network conditions. For example, after a window drop by the congestion mechanism, CogProt can keep high values for α allowing the congestion window to increase fast.

Improving the performance of the TCP protocol is a challenging issue. Results show that CogProt is able to improve average TCP performance by exploring the difference on performance for different values of α and reconfiguring TCP

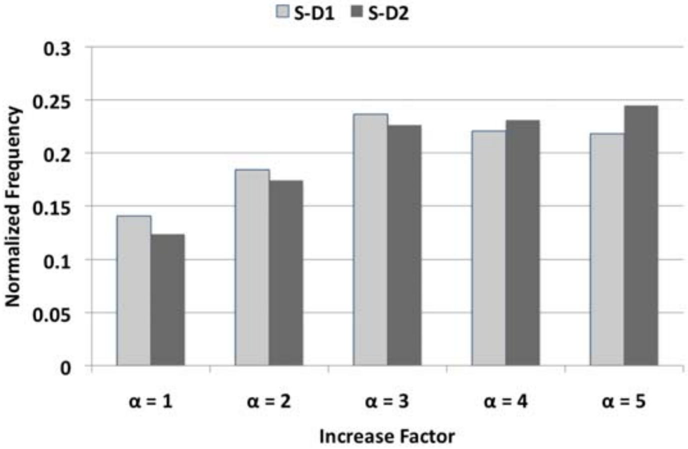


Fig. 7. Frequency of each value of α as chosen by CogProt

behavior accordingly. With any fixed value of α, TCP flows were likely to experience performance degradation for a variety of scenarios. The proposed cognitive mechanism avoids such problem. Moreover, if there are no global optimal values for a protocol parameter, CogProt can provide the best average performance by adapting the protocol to current conditions

6 Conclusion and Future Work

The proposed cognitive framework allows dynamic reconfiguration of main protocol stack parameters at different layers for achieving performance goals driven by target quality metrics. CogProt does not add a high degree of complexity and therefore it can be implemented even in network elements with limited resources. In addition, the proposed approach does not raise compatibility issues. Cognitive nodes can interoperate with ordinary nodes since the cognitive mechanism does not change protocol messages and operation.

The proposed approach was illustrated in the cognitive setting of TCP/IP reference model which brings cognitive reconfiguration into network management and protocol configuration. Performance evaluation studied the application of the proposed approach to cognitive configuration of TCP window evolution. The window increase factor is adjusted during runtime based on the TCP throughput experience achieved in the immediate past. This is a sender side only modification which constrains proper configuration of window increase factor during connection life time. It does not require any changes at the TCP receiver or any other network nodes and it is transparent to other TCP modules.

Future work will be focused on application of the proposed approach to other TCP/IP protocols as well as towards cognitive optimization algorithms distributed among network nodes. In addition, we will work on further development of architecture for the Cognitive Information Service, as well as on signaling mechanisms for cognitive information exchange between network nodes and the service and among the nodes themselves.

References

1. Akyildiz, I.F., Wang, X.: Cross-layer design in wireless mesh networks. IEEE Transactions on Vehicular Technology 57(2), 1061–1076 (2008)
2. Allman, M., Floyd, S., Partridge, C.: Increasing TCP's Initial Window. IETF RFC 3390 (Proposed Standard) (October 2002)
3. Demestichas, P., Stavroulaki, V., Boscovic, D., Lee, A., Strassner, J.: m@angel: autonomic management platform for seamless cognitive connectivity to the mobile internet. IEEE Communications Magazine 44(6), 118–127 (2006)
4. Foukalas, F., Gazis, V., Alonistioti, N.: Cross-layer design proposals for wireless mobile networks: a survey and taxonomy. IEEE Communications Surveys & Tutorials 10(1), 70–85 (2008)
5. ITU-T. Methods for subjective determination of transmission quality. ITU-T Recommendation P.800, International Telecommunication Union (ITU) (1996)
6. Mitola, J.: Cognitive radio for flexible mobile multimedia communications. Mobile Networks and Applications 6(5), 435–441 (2001)
7. Srivastava, V., Motani, M.: Cross-layer design: a survey and the road ahead. IEEE Communications Magazine 43(12), 112–119 (2005)
8. Thomas, R.W., Friend, D.H., DaSilva, L.A., Mackenzie, A.B.: Cognitive networks: adaptation and learning to achieve end-to-end performance objectives. IEEE Communications Magazine 44(12), 51–57 (2006)
9. Winter, R., Schiller, J.H., Nikaein, N., Bonnet, C.: Crosstalk: cross-layer decision support based on global knowledge. IEEE Communications Magazine 44(1), 93–99 (2006)

Topology Control in Self-managed Wireless Networks

Apostolos Kousaridas and Nancy Alonistioti

Department of Informatics and Telecommunications,
University of Athens, Athens, Greece
`{akousar,nancy}@di.uoa.gr`

Abstract. The vision for future telecommunication systems is considered as a representative example of a complex adaptive organization, where several elements, with various computational capabilities and network resources, are interconnected. The increased complexity and the continuously changing network environment make more intense the need for automation and for localized network management tasks. Self-management will allow the execution of advanced configuration actions, such as the change of the wireless network topology under various performance criteria. This paper focuses on the description of the principles and the architectural framework for the cognitive management of future communication systems, considering a complex radio access environment. This framework is used in order to present a solution on the autonomic topology control of future communication systems, where multi-hop links are established using the available relays stations, under the energy consumption constraint.

Keywords: self-management, wireless systems, cognition, topology control, relays, energy optimization.

1 Introduction

Current control and management approaches of network systems are mainly centralized, and despite their simplicity, they are resulting in many cases in bottleneck or failure points, yielding for human intervention. There is a need for new ways to control communication systems, according to new management schemes and networking techniques without neglecting the advantages of current Internet. The specification of management schemes that will enable the adaptation of network's behaviour (i.e., self-management) following de-centralized and self-organized approaches is a major challenge. Furthermore, the introduction of cognition to next generation network elements is useful for increasing the system automation by providing them the self-management capability, as well as for the improvement of their performance.

Topology adaptation at the wireless edge is considered as one of the research challenges for next generation communication systems. The (self)-management of the wireless networks topology is a key operational capability for network operators, taking into account especially dense urban network environments, consisting of various base stations, relay stations and mobile devices of high mobility. In this paper the network topology is re-organized in an automatic and distributed way for the reduction of the

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 292–301, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

energy consumption in the user equipment side, considering also the total energy consumption of the corresponding network area. The enablers that could be used in order to develop cognition and self-management capabilities are presented through the proposed Distributed Cognitive cycle for System & Network Management (DC-SNM).

The remainder of this paper is organized as follows: the related work for cognitive and self-organizing systems, which are fundamental pillars of self-managed systems, is presented in section 2. The principles and the framework for the DC-SNM are described in section 3. The process for the self-managed control of the wireless network topology for the energy consumption improvement is outlined in section 4. Finally, future research directives and conclusion are discussed in section 5.

2 Cognitive Systems and Self-organization

Cognitive systems, autonomic communications systems as well as self-organizing systems are interrelated scientific areas that are briefly surveyed in this section so as to identify functional requirements, recent advances, and proposed architectures, which attempt to establish the cognitive and adaptive behavior of computing and communication systems.

The fundamental features of an artificial cognitive system are embodiment, anticipation, adaptation, motivation, reasoning, and autonomy; these features are needed, since such architecture comprises a continue process of perception and action. Several research initiatives took place recently trying to introduce cognition in communication systems. A thorough review of artificial cognitive systems and cognitive architectures is provided by Cliff [1], D. Vernon et al. [2], and P. Langley et al. [3]. These architectures are classified into congitivist, emergent and hybrid models, taking into account their viewpoint on cognition and the different phases in cognitive science evolution. SOAR [4] and ACT-R [5], as well as SASE architecture [6] have inspired the present paper. According to Thomas et al. [7] a cognitive network bears a cognitive process that can perceive current network conditions, and then plan, decide, and act on those conditions [8]. The cognitive network can learn from these adaptations and use them to make future decisions. A framework is proposed in [9] to introduce cognition in the whole network taking into account end-to-end goals, and utilizing Software Adaptable Networks (SAN). Thomas et al. attempt to progress Mitola cognitive radio concept [10] by covering all aspects of communication networks, both wired and wireless/mobile. The introduction of cognitive capabilities in a communication system will continuously increase its intelligence, by viewing a problem in more than one ways, and by evolving its problem-solving process. In addition, the capitalization of cognition capabilities renders the system autonomous.

Apart from cognition, self-organization is another key feature of the next generation self-managed communication systems, which can be viewed as a capability that complements adaptive behavior of communication systems and contributes towards their autonomy. Self-organized systems have the capability to change their organization without any external or central dedicated control entity. Self-organization goes beyond mere distribution and may not be based on global state information [11], [12]. Multiple individual entities interact in a distributed, collaborative peer-to-peer fashion (at a microscopic level) on a common global objective, which leads to sophisticated organization and defines the behavior of the global system (at a macroscopic level), thus establishing emergent properties [13]. Self-organized systems are flexible, scalable, adaptive, robust to failures, and more reliable, since they degrade softly rather than break down suddenly. These features are necessary for future communications systems that operate in high dynamic and complex environments, considering the frequency of potential changes in their structure. Mobile Ad Hoc Networks (MANETs) and Peer-to-Peer (P2P) networks are examples of dynamic network environments, where self-organization has merit. Various algorithms and techniques have tried to solve networking issues for self-organized systems such as optimal path selection and service discovery [14].

As it is obvious from the above analysis various architectures and mechanisms for the introduction of cognitive and self-organizing capabilities have been proposed in several research fields. Thereinafter, it is necessary to transfer and adapt cognition and self-organization paradigms from other sciences or from nature to realistic use cases in communication systems, taking into account the specific characteristics of communication networks.

3 Distributed Cognitive Cycle for Network Systems Management

Future network systems design principles are based on high autonomy of network elements in order to allow distributed management, fast decisions, and continuous local optimization. The Generic Cognitive Cycle model, as it is depicted in Figure 1, is envisaged to be in the heart of Future Internet Elements (e.g., access points, base stations) and it leads to their autonomy [15], [16]. A Future Internet Element may be a network element (e.g., base station, access point, and mobile device), a network manager, or any software element that lies at the service layer. Future Internet Elements, with cognition embedded, will have a process for monitoring and perceiving network equipment's internal state and environmental conditions, and then planning, deciding and adapting (self-reconfiguring) on these conditions. Such an element is able to learn from these adaptations (reconfigurations) and use them for future decision making, while taking into account end-to-end goals.

The three distinct phases of the Generic Cognitive Cycle Model are the following:

- Monitoring process involves gathering of information about the environment and the internal state of a Future Internet Element. Moreover, the Monitoring process receives, internally or externally, information about the effectiveness of the Execution process that took place, after the last decision.
- Decision Making process includes the problem solving techniques for reconfiguration and adaptation, utilizing the developed knowledge model and situation awareness. The Decision Making supports the optimal configuration of each element, considering its hypostasis and the organization level that it belongs. Decision making mechanism identifies alternatives for adaptation or optimization and chooses the best one, based on situation assessment, understanding of the surrounding context, and the preferences of the element. After decision making, the execution process undertakes to apply the decision that will change the behaviour of the element.

- Execution process involves (self-) reconfiguration, software-component replacement or re-organization and optimisation actions.

The self-awareness of each network node is instantiated in the Knowledge Repository, which stores the necessary models that each network needs in order to describe the acquired environment, through the relative sensors and the interaction with other elements, enabling knowledge sharing. Knowledge is maintained utilizing three correlated types of memories: The semantic memory, the episodic memory and the procedural. Models about the environment, the tasks that each element supports and association of solutions at specific problems are examples of models that are available in the knowledge repository, utilizing the above memories.

Moreover the feedback (or appraisal) functionality helps the element to evaluate the result of its decision, based on problem solving experience. It assesses the result and the efficiency of an adaptation action and it is considered as as a complementary method of learning.

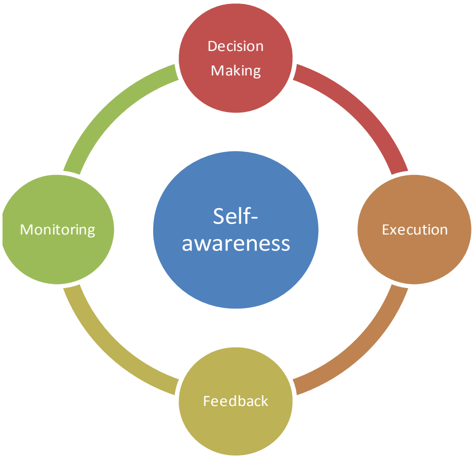


Fig. 1. Generic cognitive cycle model

A cognitive node recognizes events, and situations, and classifies them to known categories. Events recognition implies the ability to sense/monitor, to perceive objects and to interpret the environmental situation. Decision making models which solve arising problems and optimize the operation of cognitive nodes are necessary, taking into account the allowable actions and the available alternatives. Furthermore, planning and anticipation are required and are important features of an intelligent system. A plan specifies a future state description and the steps that should take place in order to achieve an identified goal or state. Anticipation mechanisms increase the intelligence of a network node, by predicting future situations as a result of certain actions on current status and facilitate problem solving because the system has the necessary time to organize and plan its actions. Moreover, reasoning methods (e.g., deduction, induction, abduction) enable a cognitive node to combine current knowledge so as to

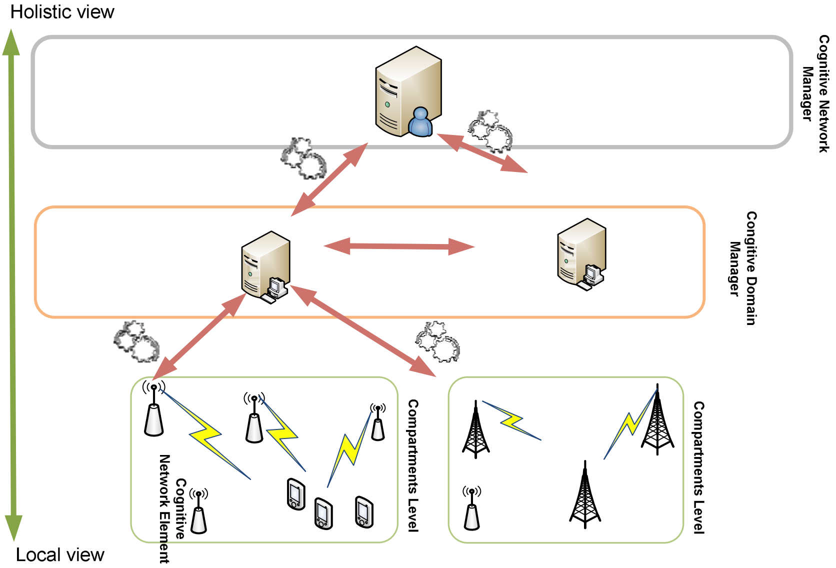


Fig. 2. Hierarchical distribution of the cognitive cycles

produce new knowledge or to draw conclusions. Learning techniques allow a cognitive node to acquire, manipulate, relate, and classify knowledge.

A Distributed Cognitive cycle for System & Network Management (DC-SNM) will facilitate the promotion of distributed/decentralised management over a hierarchical distribution of management and (re)configuration making levels to (a) (autonomic) network elements, then (b) to network domain types and (c) up to the whole network system (Figure 2). Hence, this will set the scene for one of the major design goals, which is high autonomy of network elements with cognitive capabilities aimed at fast localised (re)configuration actions and decision making. Such a distribution brings about the intriguing issue of orchestrating the cognitive cycles (M-D-E) of Monitoring, Decision Making and Executions at higher levels of the management distribution.

The logic behind the introduction of the DC-SNM is to serve as the conceptual template of introducing the Future Internet mechanisms advances in the overall system as well as a network management instrument. Hence, it is a formulated tool for addressing the complexity and capabilities of networks, services and management elements and their roles as providers of new paradigms that are emerging in the evolution of needs and mechanisms for Future Internet, service and network infrastructures in general. The Distributed Cognitive cycle for System & Network Management can be used as the guiding framework for constricting the architectural and functional features in relevant deployment scenarios.

The decomposition of network management into responsibility areas will provide the principle on which universal management architecture will be developed having as a main goal the efficient handling of complexity towards Future Internet environments. Such a decomposition combined with the introduction of cognitive functionalities at all layers will allow decisions and configuration at shorter time-scales. Each element at the identified layers has embedded cognitive cycle functionalities and also the ability to manage itself and make local decisions. For an efficient and scalable network management, where various stakeholders participate, a distributed approach is adopted. Dynamic network (re)-configuration in many cases is based on cooperative decision of various Future Internet Elements and distributed network management service components. Hints and requests/recommendations are exchanged among the layers, in order to indicate a new situation or an action for execution. The automated and dynamic incorporation of various layers requirements (e.g., SLAs) into the management aspects provides also novel features to network management capabilities. Moreover, the resolution of conflicting requests will be an issue of situation awareness and elements' domain policy prioritisation.

4 Wireless Access Systems Topology Control

Next generation wireless networks should have the capability to exploit the different advantages of cellular networks and ad hoc networks. Various types of hybrid wireless network using multi-hop approaches could be adopted in order to enrich configuration options and optimize various performance parameters. The topology of current communication systems is mainly characterized as "star topology", while future communication systems will often use relay stations (RS) with intelligent resource scheduling and cooperative transmission (i.e. not analog transmitters). Relay stations will be used in order to serve the needs of the volatile environment of future Internet wireless networks, because of user equipments' high mobility and various traffic demands. Relaying is considered as the technique to improve the coverage of high data rates, to group mobility, to deploy temporary network infrastructures, and/or to provide coverage in new areas.

Relay technologies have been recently introduced in the standardization process of both WiMAX (IEEE 801.16j [17]) and 3GPP LTE-advanced mobile systems [18]. In both cases, there are various types of relay technologies according to their implementation features. For instance, the relay transmission scheme: a) amplify and forward, b) selective decode and forward, or c) demodulation and forward that is selected affects the delay, which is introduced in the transmission and whether error propagations through the RS is avoided or not. Furthermore, with respect to the knowledge in the mobile device (MD), relays can be classified into transparent or non-transparent. It should be noted that the type of the established relay affects in many cases the performance improvement that is achieved through the activated relay station.

The minimization of the energy consumption on the MD side is another key problem that could be addressed though relay stations and which is studied in this paper. The energy consumption is a very important requirement for the end user and for the network operators in general. The distributed Cognitive Cycle for Network Systems Management vision, which has been presented in section 3, is used in order to solve locally and in a distributed way (through the involved network devices) the optimization problem of energy consumption. More specifically the M-D-E cycle is placed per base station (BS) and undertakes in collaboration with other neighboring M-D-Es that exist in the same area, to solve the energy consumption problem, which is presented and discussed below.

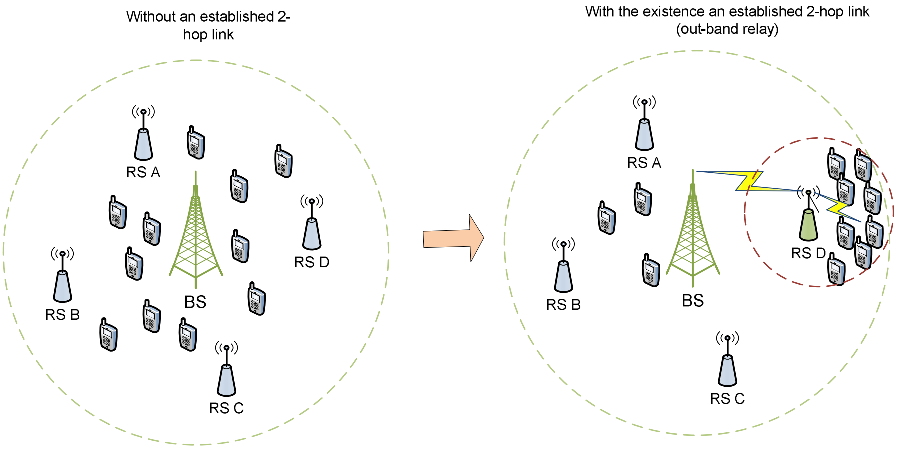

Without an established 2-hop link
With the existence an established 2-hop link (out-band relay)
RS A
RS B
RS C
RS D
BS
RS A
RS B
RS C
RS D
BS

Fig. 3. Sample wireless network topology

The base station deduces whether it is efficient to activate a relay station of a specific geographic area, as it is depicted in Figure 3, where a group of mobile devices will be transferred so as to reduce energy consumption of the latter, without on the other hand increasing the total energy consumption (including the base stations) over a specified threshold. We suppose that the RS uses an out-of-band relaying, which means that for the communication between the base station and the relay station, a different frequency is used compared to the relay station and mobile stations link. For the calculation of the energy consumption (EC) two parameters are taken into account for this use case: a) the distance between two nodes (MD, RS, BS), and b) the packet error rate (PER). The threshold is defined by the network operator, while the total energy consumption includes:

- Uplink (UL) transmissions: from the user equipment to the relay station and from the relay station to the user equipment
- Downlink (DL) transmissions: from the base station to the relay station and from the last to the user equipment.

The goal of the base station is to identify the specific opportunity to minimize the energy consumption of the user equipment (Uplink). The existence of a RS will provide to the user equipment the capability to transmit its data packet to a shorter distance, thus consuming less energy resources ($\mathrm{EC}(\mathrm{UL}_{MD\rightarrow RS})$). On the other hand, the existence of the relay (2 hops) will increase the consumed energy consumption (EC) of the network operator (BS, RS) for both the UL ($\mathrm{EC}_{Relay-enabled}(\mathrm{UL})$) and the DL ($\mathrm{EC}_{Relay-enabled}(\mathrm{DL})$). The increase of the DL energy consumption is proportional to the selected transmission range of the RS ($\mathrm{EC}(\mathrm{DL}_{RS})$). While, the increase of the energy consumption of the UL ($\mathrm{EC}_{Relay-enabled}(\mathrm{UL})$ - $\mathrm{EC}_{one-hop}(\mathrm{UL})$) is proportional to the increase of the MD-BS distance (2 hops) after the establishment of the relay. $\mathrm{EC}_{one-hop}(\mathrm{UL})$

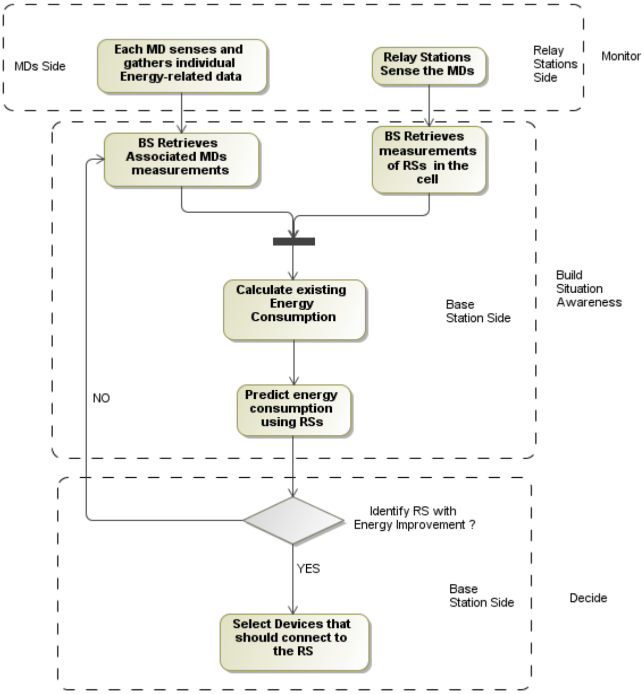

MDs Side
Each MD senses and gathers individual Energy-related data
Relay Stations Sense the MDs
Relay Stations Side
Monitor
BS Retrieves Associated MDs measurements
BS Retrieves measurements of RSs in the cell
Calculate existing Energy Consumption
Base Station Side
Build Situation Awareness
Predict energy consumption using RSs
NO
Identify RS with Energy Improvement ?
YES
Base Station Side
Decide
Select Devices that should connect to the RS

Fig. 4. Activity Diagram for the Local Topology Control

denotes the energy consumption of the UL between the MD and the BS without the usage of the relay.

Thus, the base station attempts periodically to identify if the usage of a relay station in the cell that the respective BS exists, and consequently the creation of a hop at (2-least) structure, will solve the following problem:

$$\left(\sum_{i=1}^{n}(\mathrm{EC}_{Relay-enabled}(\mathrm{UL})\text{ - }\mathrm{EC}_{one-hop}(\mathrm{UL}))+\mathrm{EC}(\mathrm{DL}_{RS})\right)<\left(\sum_{i=1}^{n}(\mathrm{EC}_{one-hop}(\mathrm{UL})-\mathrm{EC}(\mathrm{UL}_{MD\to RS}))+k\right) \quad (1)$$

where n is the number of MDs that are in the transmission range of the RS and k is the energy consumption threshold specified by the operator. This threshold is defined, by taking into consideration other benefits that the network operator will have through the activation of the relay e.g., interference reduction especially in the case of an out-of-band relaying scheme. Consequently, n is a parameter that will allow the base station that is solving the above problem, to identify the optimal solution, considering the parameter k, which is provided by the network operator.

Figure 4 presents briefly the process for the solution of the topology control for the sake of energy consumption minimization, based on the distributed M-D-E cycle. The monitoring phase takes places at the MDs (distance, PER) and RSs (sensed MDs) side, using mainly the data link layer sensing capabilities. The data are periodically transmitted to the BS (UL/DL utilization, PER), which undertakes the gathering of the measurements and proceeds to the development of its situation awareness through the calculation of the existing energy consumption levels. The BS having built the topology graph, attempts to predict using inequation (1) whether the activation of a RS (e.g., RS D, Figure 3) will decrease the energy consumption of a group of mobile devices, without increasing excessively the network side energy consumption. In the network side there is a continuous energy supply juxtaposed to the restricted energy sources (i.e. battery) of a mobile device. After the identification of the RS that satisfies inequation (1), the BS undertakes to inform the set of mobile devices that will form the 2 hops link to associate to the respective RS. The above-mentioned continuous process helps the network operators to identify optimization opportunities for their network elements (BSs, MDs), in a localized and self-organized manner.

5 Conclusions

In this paper, we proposed the exploitation of the self-management concepts through an architectural framework in order to support cognitive adaptive behavior of next generation communication system. This framework enables the development of nodes intelligence, as well as the balance between proactive and reactive adaptive behavior on the management tasks. The orchestration of the cognitive cycles as well as the distribution of their phases (e.g., monitoring) is an essential feature for realistic implementation of self-managing network systems. A network optimization use case is discussed for the energy consumption, where the available relay stations are used, and the relative signaling for the adaptation of the network topology is presented. Our ongoing work includes performance evaluation of the proposed architecture and algorithmic scheme, using specific scenarios and use cases.

Acknowledgments. This work is supported by the European Commission Seventh Framework Programme ICT-2008-224344 through the Self-NET Project (https://www.ict-selfnet.eu).

References

1. Cliff, D.: Biologically-Inspired Computing Approaches To Cognitive Systems: a partial tour of the literature. Technical Report, `http://www.hpl.hp.com/techreports/2003/HPL-2003-11.html`
2. Vernon, D., Metta, G., Sandini, G.: A Survey of Artificial Cognitive Systems: Implications for the Autonomous Development of Mental Capabilities in Computational Agents. IEEE Transactions on Evolutionary Computation, Special Issue on Autonomous Mental Development (2007)
3. Langley, P., Laird, J.E., Rogers, S.: Cognitive architectures: Research issues and challenges (2006), `http://cll.stanford.edu/~langley/papers/final.arch.pdf`
4. SOAR, `http://sitemaker.umich.edu/soar/home`
5. ACT-R, `http://act-r.psy.cmu.edu`
6. Weng, J.: On Developmental Mental Architectures. Neurocomputing 170(13-15), 2303–2323 (2007)

7. Thomas, R.W., DaSilva, L.A., MacKenzie, A.B.: Cognitive networks: adaptation and learning to achieve end-to-end performance objectives. IEEE Communications Magazine 44(12), 51–57 (2006)
8. Haykin, S.: Cognitive radio: brain-empowered wireless communications. IEEE Journal on Selected Areas in Communications 23(2), 201–220 (2005)
9. Thomas, R.W., DaSilva, L.A., MacKenzie, A.B.: Cognitive networks. In: First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pp. 352–360 (2005)
10. Mitola III, J., Maguire Jr., G.Q.: Cognitive radio: Making software radios more personal. IEEE Personal Communications 6(4), 13–18 (1999)
11. Prehofer, C., Bettstetter, C.: Self-organization in communication networks: principles and design paradigms. IEEE Communication Magazine 43(7), 78–85 (2005)
12. Bogenfeld, E., Gaspard, I.: Self-x in Radio Access Networks, E3 White Paper (2008), `https://ict-e3.eu/project/white_papers/Self-x_WhitePaper_Final_v1.0.pdf`
13. Dressler, F.: Self-Organization in Ad Hoc Networks: Overview and Classification, University of Erlangen, Dept. of Computer Science 7, Technical Report 02/06 (March 2006)
14. Biskupski, B., Dowling, J., Sacha, J.: Properties and mechanisms of self-organizing MANET and P2P systems. ACM Transactions on Autonomous and Adaptive Systems (TAAS) 2(1) (2007)
15. Kousaridas, A., Polychronopoulos, C., Alonistioti, N., Marikar, A., Mödeker, J., Mihailovic, A., Agapiou, G., Chochliouros, I., Heliotis, G.: Future internet elements: cognition and self-management design issues. In: Proceedings of the 2nd International Conference on Autonomic Computing and Communication Systems, Turin, Italy, September 23 - 25 (2008)
16. Kousaridas, A., Alonistioti, N.: On a synergetic architecture for cognitive adaptive behavior of future communication systems, International Symposium on World of Wireless.In: Mobile and Multimedia Networks (WoWMoM), pp. 1–7 (2008)
17. IEEE P802.16j, EEE Draft Amendment to IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Multihop Relay Specification (2009)
18. 3GPP TR 36.814 V1.5.0, Further advancements for E-UTRA Physical layer aspects, Tech. Spec. Group Radio Access Network (December 2009)

Autonomicity and Self-manageability Techniques in the Scope of the Future Internet's Evolution

Ioannis P. Chochliouros[1], Anastasia S. Spiliopoulou[2], Maria Belesioti[1], Evangelos Sfakianakis[1], George Diakonikolaou[1], Andreas Rigas[1], Evangelia Georgiadou[1], George Agapiou[1], and Tilemachos Doukoglou[1]

[1] Hellenic Telecommunications Organization (O.T.E.) S.A.,
Research Programs Section, Labs & New Technologies Division,
Pelika & Spartis Street, 15122 Maroussi, Athens, Greece
{ichochliouros,mbelesioti,esfak,gdiako,arigas,egeorgiadou,
gagapiou,tdouk}@oteresearch.gr
[2] Hellenic Telecommunications Organization (O.T.E.) S.A.,
General Directorate for Regulatory Affairs,
99, Kifissias Avenue, 15124 Maroussi, Athens, Greece
aspiliopoul@ote.gr

Abstract. Upon the basis of the essential principles characterizing the development towards the establishment of the Future Internet (FI), the paper discusses innovative aspects for autonomicity and self-manageability, as the latter are introduced by the context of the Self-NET Project effort. We identify the "core" issues for a modern network management activity and related capabilities, incorporated in appropriate network elements/domains (and/or in clusters of them), by considering a novel feedback-control cycle, known as the MDE cognitive cycle. We discuss several major benefits originating from such an innovative approach. Self-NET develops self-management features that alleviate consequences of events for which the system would require various invocations of remedy actions and/or human intervention.

Keywords: Autonomic communications, cognitive networks, Future Internet, generic cognitive cycle model, network management, self-management.

1 Introduction

The Internet has been identified as one of the most critical infrastructures of the 21st century, sustaining social and economic evolution, *just as railways, roads and aeronautic transport networks have been doing over the past century*. It is not simply the "*vehicle*" of a modern services-based economy, *but also a tool to support the appearance of the "fifth freedom" and a truly knowledge-based society* [1]. The transformation the Internet has brought to modern economies and societies will be more apparent in the future, driven by the growth of Information and Communication Technologies (ICT) [2] and by the blossoming of novel business and societal applications [3]. There is a broad consensus that the Internet, *as it is perceived today,* challenges traditional regulatory theories and governance practices. But as the future of the Internet comes

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 302–317, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

into consideration, even greater challenges are seen, with many questions related to privacy, security and governance and with a variety of issues related to Internet's effectiveness and inclusive character [4]. Future relevant applications will attract more users to novel services needing greater mobility, wider bandwidth, higher speeds and enhanced interactivity through the launch of many new interactive media and content services [5]. Such demands, *however*, implicate challenges for a more secure, reliable, and scalable Internet architecture. Effectively deployed, the Internet of the future can bring novelty, productivity gains, new markets and growth. In fact, innovative functionalities with more enhanced performance levels are necessary to sustain the real-time requirements of a multitude of novel applications. Furthermore, the Internet underpins the whole global economy. The networking effect has made possible an accelerated and universal diffusion of innovation. The diversity and sheer number of applications and business models supported by the Internet have also largely affected its nature and structure [6]. The Internet is evolving both in its use and in its technology. Born from the vision to create an "open infrastructure" to network computers across the world, the Internet has become a socio-economic backbone of our society, with countless private and business users as well as governments relying on it on a daily basis. The "drivers" for this evolution are a mixture of emerging players with diverse and potentially changing interests, be it users, operators, manufacturers, service and content providers, together with advances in technology that have become available over the years [7].

The ***Future Internet (FI)*** will not be "more of the same", but rather an infrastructure that incorporates new technologies on a large scale that can unleash novel classes of applications and related business models ([8], [9]). If today's Internet is a crucial element of our economy – the Future Internet will play an even more vital role in every conceivable business process. It will become the productivity tool "*par excellence*" [10]. At present, there are many so called "*Future Internet*" initiatives around the world working on defining and implementing a new architecture for the Internet intended to overcome existing limitations mostly in the area of networking [11]. Beyond technological issues, the restructuring of business and social interaction processes unleashed by the Future Internet infrastructure could provide European stakeholders with a golden opportunity to lead a new wave of innovation and to establish a position in the Internet economy that is commensurate with their technological and scientific know-how [12].

Europe remains a global force in advanced information and communication technologies and has massively adopted broadband and Internet services ([13], [14]). The European Union (EU) is actually a potential leader in the Future Internet sector [15]. Leveraging Future Internet technologies through their use in "smart infrastructures" offer the opportunity to boost European competitiveness in nascent technologies and systems, and will make it possible to measure, monitor and process huge volumes of information. This can also provide the means to "overcome" fragmentation and to build a relevant critical mass at European level, while fostering competition, openness and standardisation, involving consumer/citizen, ensuring trust, security and data protection with transparent and democratic governance and control of offered services as guiding principles [16]. The current policy environment for the Internet-based economy is affected by three essential trends, i.e. convergence, creativity and confidence ([17], [18]).

2 Network Management Capabilities in the Future Internet

Innovation, the foundation for economic development, depends on rapid scientific advances. The face of the Internet is continually changing, as new services and novel applications appear and become globally noteworthy at an increasing pace, while new and traditional players are adapting to these challenges through new business models [19]. The current Internet has been founded on a basic architectural premise, that is: *a simple network service can be used as a "universal means" to interconnect intelligent end systems* [20]. The current Internet is centered on the network layer being capable of dynamically selecting a path from the originating source of a packet to its ultimate destination, with no guarantees of packet delivery or traffic characteristics. The end-to-end argument has served to maintain the desire for this simplicity. It is now a common belief that the current Internet is reaching both its architectural capability and its capacity limits (i.e. addressing, reachability, new demands on quality of service (QoS), service/application provisioning, etc). The next generation network architecture will fix the shortcomings of the current Internet, including s*ecurity, privacy, trust and identity management*. It will have "hooks" for business and incentive models, support for semantics, support for mobility, and it will be resilient. This architecture will be flexible enough to support a range of application visions and business models in a dynamic way, ensuring convergence between technology, business and regulatory concerns. New communication technology will enable increasing connectivity, through both wired and wireless communication, both near-range and far-range. Enhanced communication services will open many possibilities for innovative applications that are not even envisioned today. Challenges for the Network of the Future may refer to a great variety of factors, including but not limited to: Dependability and security; transparency (trust); scalability; services (i.e.: cost, service-driven configuration, simplified composition of services over heterogeneous networks, large scale and dynamic multi-service coexistence, exposable service offerings/catalogues); monitoring, reporting and auditability capacities; accounting and billing; Service Level Agreements (SLAs) and protocol support for bandwidth (dynamic resource allocation), latency and QoS; automation (e.g. automated negotiation/instantiation); autonomicity, and; harmonization of interfaces. The resolution of these challenges would bring benefits to infrastructure/network providers, in terms of: Simplified contracting of new business; establishing/identifying reference points for resource allocation and re-allocation; enabling flexibility in the provisioning and utilization of resources; offering the ability to scale horizontally, and; providing a natural complement to the virtualization of resources -by setting up and tearing down composed services, based on negotiated SLAs- thus simplifying accounting and revenue tracking. This can also implicate benefits for service providers/consumers, in terms of: Ready identification and/or selection of offerings; the potential to automate the negotiation of SLA Key Performance Indicators (KPIs) and pricing; reduced cost and time-to-market for composed services; scalability of composed services, and; flexibility and independence from the underlying network details.

A current trend for networks is that they are becoming service-aware. Service awareness itself has many aspects, including the delivery of content and service logic, fulfillment of business and other service characteristics such as QoS and SLAs and the optimization of the network resources during the service delivery. Thus, the design of Networks and Services is moving forward to include higher levels of automation, autonomicity, including self-management. Conversely, services themselves are becoming network-aware. Manageability of the current network typically resides in client stations and servers, which interact with network elements (NEs) via protocols such as SNMP (Simple Network Management Protocol). The limitations of this approach are reduced scaling properties to large networks, and the need for extensive human supervision and intervention. A new network manageability paradigm is thus needed that allows NEs to be autonomously interrelated and controlled, that adapts dynamically to changing environments, and that learns the desired behavior over time. The effective design of monitoring protocols so as to support detection mechanisms critical for the elaboration of self-organizing networks has to be based on a clear understanding of engineering "trade-offs" with respect to local vs. non-local and aggregated information, *for instance*. (Possible techniques for realizing such protocols include distributed tree algorithms, gossip algorithms and stochastic models). Several issues identified in current network infrastructures impose the need for the introduction of an innovative architectural design. More specifically, existing web-based service front-ends are based on monolithic, inflexible, non-context- aware user interfaces (UIs). Furthermore, the diversity of services as well as the underlying hardware and software resources constitute management issues highly challenging, meaning that currently, a diversity in terms of hardware resources leads to a diversity of management tools (distinguished per vendor). In addition, security risks currently present in network environments request for immediate attention. This could be achieved by building trustworthy network environments (as well as communication, computing and storage infrastructures) to assure security levels and manage threats in interoperable frameworks for autonomous monitoring. Another important factor necessitating the need for dynamic FI environments is the reduction of "time to market", referring to the provision of services designated for the end users.

FI's vision, is of a self-managing network whose nodes/devices are designed/ engineered in such a way that all the so-called traditional network management functions, defined by the "*FCAPS*" management framework (Fault, Configuration, Accounting, Performance and Security) [21], as well as the fundamental network functions such as routing, forwarding, monitoring, discovery, fault-detection and fault-removal, are made to automatically feed each other with information (i.e. "knowledge") such as goals and events, in order to effect feedback processes among the diverse functions. These feedback processes enable reactions of various functions in the network and/or individual nodes/devices, in order to achieve and maintain well defined network goals ([22], [23]). Self-management capabilities may relate to a great variety of essential issues, including but mot limited to: (i) Cross-domain management functions, for networks, services, content, together with the design of cooperative systems providing integrated management functionality of system lifecycle, self-functionality, SLA, and QoS; (ii) Embedded management functionality in all FI systems, such as in-infrastructure management, in-network management, in-service management, and in-content management; (iii) Mechanisms for dynamic deployment of new management functionality without interruption of running FI systems; (iv) Mechanisms for dynamic deployment of measuring and monitoring probes for services' and network' behaviors, including traffic. This also implicates SLA-aware sensing and continuous monitoring of systems' adaptations, together with the use of monitoring services in support of the self-management functionality; (v) Mechanisms for conflict and integrity-issues detection and resolution across multiple self-management functions; (vi) Mechanisms, tools and methodology for the verification and assurance of different self-capabilities that are guiding systems and their adaptations correctly; these can also relate to mechanisms for allocation and negotiation of different resources; (vii) Increased level of self-awareness, self-knowledge, self-assessment and self-management capabilities for all Future Internet systems, services, and resources; (viii) Increased level of self-adaptation and self-composition of resources to achieve effective, autonomic and controllable behavior; (ix) Increased level of self-contextualization and context-awareness for network and service systems and resources; (x) Increased level of resource management, including discovery, configuration, deployment, utilization, control and maintenance; (xi) Self-awareness capabilities to support system-level objectives of minimizing system life-cycle costs and energy footprints; (xii) Orchestration and integration of management functions, i.e. a service-driven dynamic orchestration, and; (xiii) Capabilities for the control relationships between self-management and self -governance of the Future Internet.

In such an evolving environment, *it is required the network itself to help detect, diagnose and repair failures, as well as to constantly adapt its configuration and optimize its performance*. Looking at ***Autonomicity and Self-Manageability,*** autonomicity (i.e. control-loops and feed-back mechanisms and processes, as well as the information/knowledge flow used to drive control-loops), becomes an enabler for self-manageability of networks [24]. Suitable equipments and/or systems with communication and computational capabilities can be integrated into the fabric of the Internet, providing an accurate reflection of the real world, delivering fine-grained information and enabling almost real time interaction between the virtual world and real world. In particular, autonomous self-organizing systems are beginning to emerge and to be widely established [25]. Such systems "*can adapt autonomously*" to changing requirements and reduce the reliance on centrally planned services, *especially if they are joined with new network management techniques* [26]. Operators may use these tools to guarantee good QoS service in a period of exploding demand and rising network congestion at peak times. The trend in building dependable real-life systems and smart infrastructures today is "*to move from monolithic, centralized and strictly hierarchical systems to highly distributed networked systems with local and global autonomy*". Some of the challenges for operators and service providers include management (especially in self-organized wireless environments), resilience and robustness, automated re-allocation of resources, abstractions of the operations in the underlying infrastructure, QoS guarantees for bundled services and the optimization of operational expenditures (OPEX). The requirement of a single, scalable and configurable architecture is an essential one of the driving forces for the FI [27]. The variety and heterogeneity of the emerging business models, as well as the dynamic service composition and provision may lead to a situation of many Internets, with different architectural structure, requirements and functionality. Such a scenario will result in a nightmare of maintenance efforts, increased costs, incompatibilities and the like. It is thus important to try to build a single core architecture that maintains properties like configurability, extendibility, scalability and openness. Keeping the core architecture as generic as possible will offer the possibility to easily extend and adapt it to the requirements of the edge. Such a design will follow the rising trend of moving intelligence to the edge of the network.

Nowadays computing systems are open systems evolving in a dynamic complex environment. They are designed as sets of interacting components, highly distributed both conceptually and physically. The growing complexity of these systems and their large scale distribution [28] make the use of traditional approaches based on hierarchical functional decomposition and centralised control no more applicable. Several among the existing technology systems are desired to sufficiently "exhibit" interesting characteristics, such as robustness, capacity of self-management and self-adaptation, as well as survivability in uncertain and dynamic environments. Ubiquitous and self-organizing systems are not only disruptive technologies that impact the way how market actors organize core processes as well as existing structures in value chains and industry, but have also considerable impact [29]. The present Internet model is based on clear separation of concerns between protocol layers, with intelligence moved to the edges, and with the existent protocol pool targeting user and control plane operations with less emphasis on management tasks [30]. The area of FI is considered as a representative example of a "*complex adaptive organization*" (or "*entity*"), where the involved partners have conflicting goals and tension to maximize their gains. Among the core drivers for the Future Internet are increased reliability, enhanced services, more flexibility, and simplified operation. The latter calls for including ***Network Management***[1] ***(NM)*** issues into the design process for FI principles. (In general NM is a service (or application) that employs a diversity of tools, applications, and devices to assist human network managers in monitoring and maintaining networks Thus, network management should be an integral part of the future network infrastructure. Management is a key factor in manageability, usability, performance, etc., and is an important factor to the operational costs of any "network entity". FI requires a new management approach, promoted mainly by the necessity of support interoperability between heterogeneous, complex and distributed systems. In addition, FI should remain open for further and continuous improvement, without the necessity of another disruptive modification in the future. Furthermore, as network management is important for the reliable and safe operation of networks, it is also crucial for the success of the FI. In the scope of these challenges, the ***Self-NET Project*** [31] aims to integrate the self-management and cognition features and the inevitable part of FI evolution [32].

3 The Context of the Self-NET Approach

The novelty factors introduced by cognitive networks appear in a variety of sectors. In particular, the incorporation of a certain degree of intelligence in the network includes an increased capability on a "per element" basis, in terms of monitoring, decision making and execution aspects. Moreover, network nodes themselves can "learn and act" without the need for centralized management mechanisms. Consequently, network environments become more flexible as they are reinforced with self-aware elements, automatic topology discovery mechanisms and several dynamic cross-layer adaptation functionalities. Moreover, dynamic and optimal allocation of resources can

---

[1] In general, NM is a service (or application) that employs a diversity of tools, applications, and devices to assist human network managers in monitoring and maintaining networks.

be taken into account as a highly significant challenge that could be addressed through novel cognitive networking infrastructures.

The Self-NET Project aims to design, develop and validate an innovative paradigm for cognitive self-managed elements of the Future Internet. The present Internet model is based on clear separation of concerns between protocol layers, with intelligence moved to the edges, and with the existent protocol pool targeting user and control plane operations with less emphasis on management tasks. Self-NET intends to engineer the Future Internet based on cognitive behavior with a high degree of autonomy, by proposing and examining the operation of self-managed Future Internet elements around a novel "feedback-control cycle" (i.e. the "Monitoring/Decision-Making/Execution" or "MDE" cycle) [33]. Thus, dynamic distribution of resources according to network needs at specific time intervals can be pursued by introducing the "MDE" cycle in order to overcome bottlenecks and ensure seamless service provisioning – *even in case of services with high bandwidth requirements*. The completion of the aforementioned objective can make certain better QoS, *beyond the original best-effort status,* and simultaneously eases operational and network management functionalities. Cognitive management in FI elements introduces also innovative techniques regarding converged infrastructures with ultra-high capacity optical transport/access networks and converged service capability across heterogeneous environments.

Self-NET principle design is based on high autonomy of network elements in order to allow distributed management, fast decisions, and continuous local optimization either of existing networks or of specific network parts [34]. The three distinct phases of the Generic Cognitive Cycle Model-GCCM (i.e. the MDE cycle) are the following ones (as illustrated in Fig.1): (i) The ***Monitoring*** *process* which involves gathering of information about the surrounding environment (which can be a complex clustering of several NEs, broader infrastructures and/or related facilities) and the internal state of a Future Internet element; (ii) The ***Decision-Making*** *process* which includes learning, knowledge building and decision-making for reconfiguration and adaptation, by utilizing the developed knowledge model and situation awareness (SA); (iii) The ***Execution*** *process* which involves (self-) reconfiguration, software-component replacement or re-organization and (selected) optimization actions. The Monitoring process receives, *internally or externally*, information about the effectiveness of the Execution process that took place, after the last decision. The Execution and Monitoring interaction is considered as an "*indirect feedback*", useful for system's learning process and, *in sequel*, for the update of the knowledge model. In particular, the Generic Cognitive Cycle model is envisaged to be in the heart of FI Elements [35]. A FI "Element" may be a NE (e.g., router, base station (BS), and mobile device), a network manager, or any software element that lies at the service layer. Future Internet Elements, with cognition embedded [36], will have a process for monitoring and perceiving internal and environmental conditions, and then planning, deciding and adapting (i.e. "self-reconfiguring") on these conditions [12]. Such an "element" is able to "*learn*" (or "*to extract knowledge*") from these adaptations (reconfigurations) and use them for future decision making, while taking into account end-to-end goals, as implied by the considered network infrastructure.

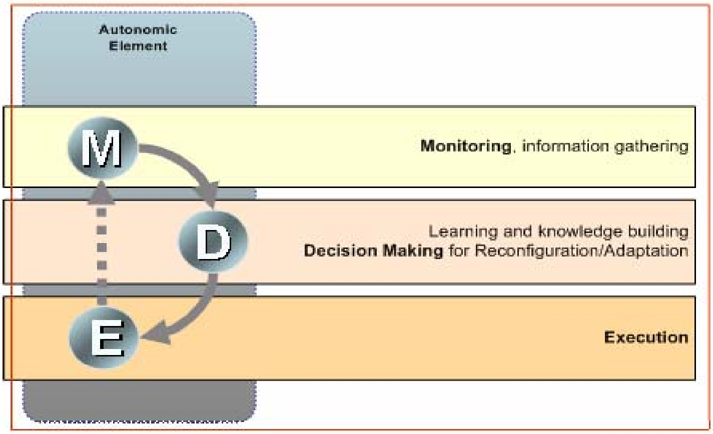

Autonomic Element
M
D
E
Monitoring, information gathering
Learning and knowledge building
Decision Making for Reconfiguration/Adaptation
Execution

Fig. 1. The Generic Cognitive Cycle Model applied in the Self-NET Context

Cognitive capabilities can enable the perception of the NEs environment and the decision upon the necessary action (e.g. configuration, healing, protection measures, etc.). As current management tasks are becoming overwhelming, Self-NET intends to embed new management capabilities into NEs in order to take advantage of the increasing knowledge that characterizes the daily operation of mobile FI users. Among the main Self-NET's efforts is "*to tackle complexity*" by following the well-known "divide and conquer" approach, that is by: "*Breaking down the overall network management task into smaller manageable tasks and assigning them to individual network elements*"; showing NEs how to tackle the relevant issues; giving NEs the ability to "learn" in order to solve new, emerging (and occasionally "unforeseen") problems; facilitating NEs to cooperatively solve problems that require a sort of coordination, and; enhancing Future Internet with inherent management capabilities *(i.e. "making FI self-manageable").* NEs with cognitive capabilities aim at fast localised decision making and (re-) configuration actions as well as learning capabilities that improve elements behavior. Furthermore, Self-NET intends to provide a peer-to-peer style distribution of responsibilities among self-governed elements of the FI, therefore overcoming the barrier of current client-server and proxy-based models in the operation of mobility management, broadcast/multicast, and QoS mechanisms. A Self-Net's "key-objective" is the provision of a holistic architectural and validation framework that unifies networking operations and service facilities of the FI [37].

FI design is required to provide answers to a number of current Internet's deficits, especially when the danger of increased complexity is more than evident. ***Self-management and autonomic capabilities*** can alleviate this "drawback" by: Providing inherent management capabilities; increasing flexibility, and; allowing an ever-evolving Internet. Towards realizing this aim, the Self-NET Project considers a Distributed Cognitive cycle for System & Network Management (DC-SNM) along with a hierarchical distribution over the network can map self-management capabilities over Future Internet architecture [38]. DC-SNM will further facilitate the promotion of distributed/decentralized management over a hierarchical distribution of management and (re)configuration making levels: (a) to (autonomic) network elements; (b) to network domain types, and; (c) up to the service provider realm, hence allowing high autonomy of network elements with cognitive capabilities aimed at fast localised (re)configuration actions and decision making. Such a distribution brings about the intriguing issue of orchestrating the cognitive cycles (M-D-E) at higher levels of the self-management distribution. The "*decomposition*" of network management into responsibility areas (as shown in Fig.2) can provide the principle on which universal management architecture will be developed, having as a main goal the efficient handling of complexity towards FI environments ([39], [40]).

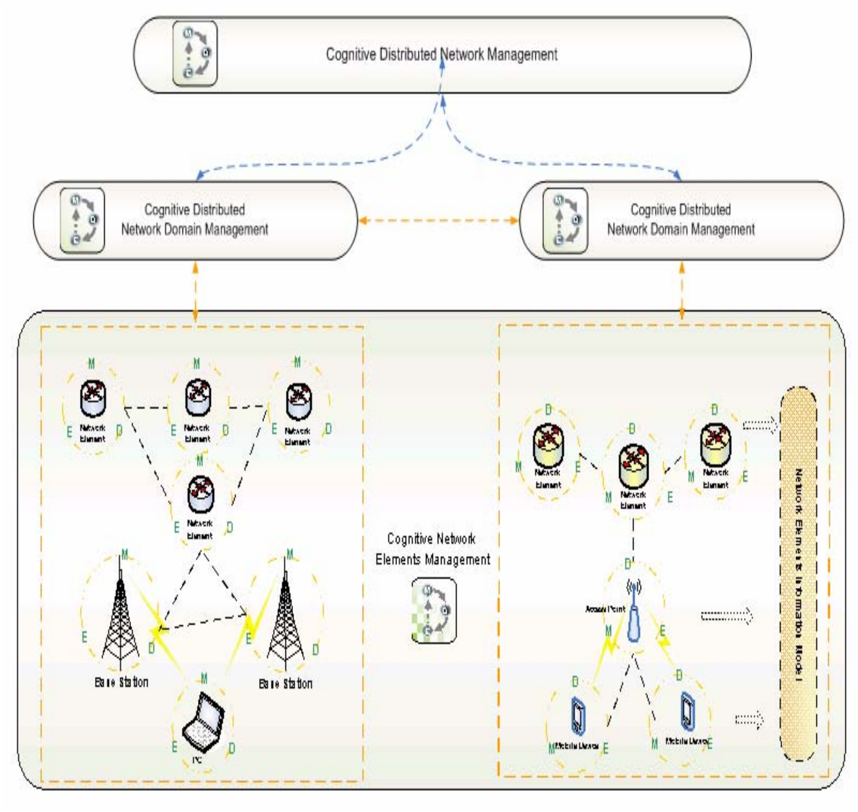

Cognitive Distributed Network Management
Cognitive Distributed Network Domain Management
Cognitive Distributed Network Domain Management
Network Element
Base Station
Base Station
PC
Cognitive Network Elements Management
Access Point
Mobile Device
Mobile Device
Network Elements Information Model
M
D
E

Fig. 2. The proposed Distributed Cognitive Cycle for Systems and Network Management (DC-SNM) purposes

Each element at the identified layers has embedded cognitive cycle functionalities and also the ability to manage itself and make appropriate local decisions. Dynamic network (re-)configuration in many cases is based on cooperative decision of various FI elements and distributed NM service components [41]. Hints and requests/recommendations are exchanged among the corresponding layers, in order to "indicate" (or to identify) a new situation or an action for targeted execution. The automated and dynamic incorporation of various layers requirements (e.g., SLAs (service level agreements)) into the management aspects provides also novel features to NM capabilities. Moreover, the resolution of conflicting requests will be an issue of situation awareness and elements' domain policy prioritization [42]. In the context of the Self-NET Project, the introduction of a hierarchical Cognitive Cycle to enable multi-tier self-management in various network elements and dynamic network compartments provides a quite promising approach to alleviate management overhead, ensure dynamic adaptation to service requirements, situation aware NM and reconfiguration, while coping with the fragmentation of contemporary centralised network management dedicated to specific types of networks [43]. For businesses of all sizes, it is imperative to consider a NM solution that is easy to use, quick to deploy, and offers low total cost of ownership [44]. Such a solution implicates comprehensive capabilities and a satisfactory reliability. The adoption of appropriate cognitive techniques on different platforms (and/or on parts of them, also including connected devices) can be the "kick-off" that will encourage the creation of new networking infrastructures. This implicates several distinct advantages and/or expected benefits, as the latter have been discussed in the scope of previous Self-NET based works [38]. Although there is a diversity of external and influencing available definition on self-management related work ([45], [46]), the term ***"self-management"*** is applied here as the general term describing all autonomic and cognition-based operations in a system. Six relevant distinct methods are identified with specific realizations and purposes; they all serve to demonstrate principles and concepts inherent in the system properties, for achieving completeness and accuracy.

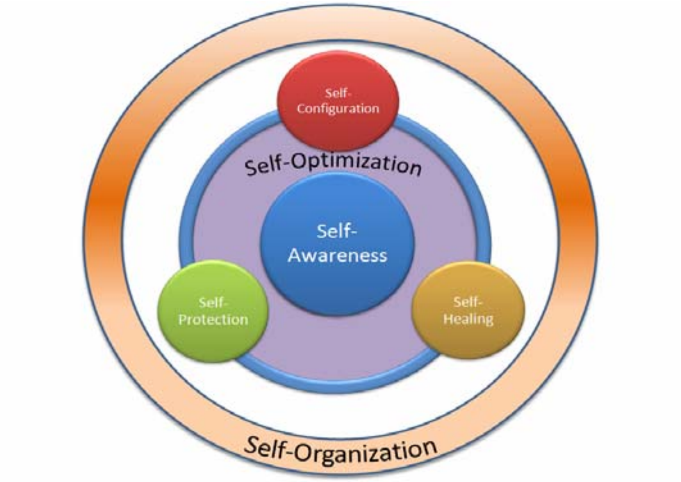


Fig. 3. Definition of the proposed self-management methods

These methods differ in terms of the perspectives on how the systems invoke executions and relevance to the detection processes; they are all depicted in Fig. 3 and defined as follows: (i) ***Self-awareness*** represents the knowledge-building process as a continuous necessity in self-management systems, and it is perceived as "*conclusions derived by the system on being present in a particular operational state (or status) at* *a given time-frame*". (ii) ***Self-optimization*** is system's ability to execute modifications of its operations for attaining the targeted "*optimality point*"[2] in terms of the related performance metrics for a given event. (iii) ***Self-configuration*** is system's ability to accommodate/incorporate new operational aspects in terms of NEs, hardware, software, functional improvements and services that have been provisioned by the operator. The essence of this method is in having the ability to "*add*" and "accommodate" new functional components; (iv) ***Self-healing*** is system's ability to react to unplanned events (such as failures) requiring corrective actions (or countermeasures) and, *accordingly*, to restore or "improve" its operational aspects. The method is rather diverse in terms of the targeted operational aspects that are affected, as this is relevant to the degree of the "healing" required; (v) ***Self-protection*** is system's ability to compensate effects of foreseen events or overcome them completely in terms of their impact on its operational aspects. This is perceived in using the gathered knowledge for deducing the events in advance to their occurrence and then proactively directing specific operations. Emphasis is put on the proactive nature of the system and can also be generalised to identification of external attacks, for which the system's detection process may follow similar pattern(s) of gathering knowledge (but can be overlapping with self-healing in some cases); (vi) ***Self-organisation*** is a specific method indicating ways of collaborations of NEs (or clusters of them) in the context of specific management functions. All the previous self-management definitions specify a broad range of discipline that might be present in self-managed/cognitive systems in FI networks and a diversity of occurrences that can trigger invocations of self-management processes.

4 Benefits Originating from Cognitive Network Management

The adoption of cognitive techniques on different platforms and devices can be the "kick-off" to encourage the creation of new networking infrastructure [47]. For operators and users, the benefits of the introduced Self-NET functionalities in Internet-based architectures can include *inter-alia*:

Automatic planning and reduction of management time of complex network parameters and structures: The current and future anticipated high proliferation of different services that a communications network should support, places a very challenging issue for network operators to solve, and makes the tasks of adjusting network performance and optimizing network resource usage as critically important. Daily (human) network manager activities consist of numerous tedious and time-consuming tasks in order to ensure that the network delivers the desired services to its users. Embedding self-management functionalities in future NEs and introducing cognition in the various network levels (e.g., network elements, network compartments, and network domains) can automate the detection of unusual (or undesirable) behavior, the isolation of their sources, the diagnosis of the corresponding fault(s) and the expected repair of the problem. In some cases, it is also desirable to actually predict

---

[2] The "optimality point" is considered as a broader term, including a variety of parameters all subject to particular types of events in the system and it is related to the evaluation criteria applied by the involved functionality.

irregular events (like faults or intrusions) and to react, *accordingly*, in due time, as the vulnerability of NEs remains a critical issue for network operators. Applying self-aware techniques in a network environment can thus ease network composition and planning procedures and ensure automatic adaptation of networks and services to the current capabilities of the network components.

Operational costs reduction: Any infrastructure capable of performing automated operational tasks for the aim of optimization of both network efficiency and service quality, can so contribute to the objective of reducing actual network operational expenditures (OPEX). This also enables a more affordable and simpler network deployment. By applying self-management techniques aiming at optimizing the network in terms of coverage, capacity, performance etc., operators can decrease their operational expenditures by reducing the manual effort required to operate a network and can utilize their network elements/resources more efficiently. Furthermore, such techniques can also simplify network maintenance and fault management, by reducing related costs, as well.

Easy adaptation of networks (e.g., in new traffic models and schemes): Traditional traffic management of a communications network usually relies on integrated and centrally coordinated deployment of measures and rules, in response to the current network operating state and/or in anticipation of future needs and traffic conditions. Traffic management configuration of large wireless networks that consist of multiple, distributed NEs of varying technologies is challenging, time-consuming, prone to possible errors and requires highly expensive control & management equipment from any operator. Even when it is initially deployed, it requires continuous upgrades and related modifications so that to provide a uniform and transparent service environment, to sustain high QoS, to recover from faults and to maximize the overall network performance, especially when congestion happens.

Seamless experience to users in selecting a network in a dynamic and robust manner: It is a matter of major importance, for the end-users, to have access to a network providing coverage and services of high quality, on a real-time basis. Self-management techniques imply decentralized monitoring and decision-making procedures so that suitable optimization hints can be extracted in terms of determining the optimum course of actions in order to improve network performance and stability and guarantee service continuity to the users.

Improved service provision and adaptability: Any dynamic detection of operational deficiencies or poor QoS delivered to the end-user, both imply specific remediate actions to be performed, so that to compensate for the related identified problems. Improving the overall network quality also increases subscribers' satisfaction. The optimization of procedures in order to minimize (or even to "*delete*") service failures and to ensure the continuity of service delivery in a network environment, is a matter of major importance for the user and the operator, in a competitive and liberalized telecommunications market.

To enable effective and efficient networking under highly demanding conditions, a continuous NM (proactively and reactively adapted to the network dynamics) is necessary. Instead of using manual techniques, a fully automated, transparent and intelligent traffic management functionality can be much more beneficial. The suggested Self-NET infrastructure can so be used to provide efficient real-time traffic management in a large network, maximizing network performance and dramatically decreasing human intervention. Particular application areas can cover cases of traffic congestion [48], network attachments, link failures, performance degradation, mobility issues, multi-service delivery enhancements and involve intelligent autonomic congestion management and traffic routing, dynamic bandwidth allocation and dynamic spectrum re-allocation [37]. The continuity of service availability influences directly the technical approach of service realization and is an important parameter affecting the planning of the network, so the latter should have the appropriate techniques to "*adapt itself*" to an essential (occasionally prescribed) functional state. The application of self-aware mechanisms can lead to network performance optimization in terms of coverage and capacity, optimization of QoS delivered to the end-user, reduction of human intervention in terms of determining the most appropriate course of actions and proceeding to the implementation of optimization activities. Applying self-aware mechanisms in future networks will contribute towards guaranteeing the following critical features: (i) High availability and seamless continuity of services; (ii) Connectivity anywhere and anytime; (iii) Robustness and stability of the underlying network infrastructure; (iv) Scalability in terms of features and functions; (v) Optimal balance between cost network-related benefits (OPEX reduction – optimized network functionalities), and; (vi) Support for heterogeneity in terms of system components and services.

5 Conclusion

Evolution towards Future Internet imposes the need of building a more flexible and resilient architecture that will serve as the basis for the provision of a diversity of services with optimized quality levels, aiming to the attraction of end users and ensuring at the same time a high degree of satisfaction. Cognitive networks and self-aware functionalities introduce a great degree of autonomy, meaning that embedded and inherent management functionality in several components of FI systems constitute management a "*per NE*" and "*per domain*" mechanism rather than a centralized network functionality. Compared to current networks, self-management techniques pave the way towards automating processes such as the deployment of new NEs, selection and execution of the optimal solution based on specific circumstances and remediation of identified malfunctions with minimum service interruption. New methods (related to embedded and autonomous management, virtualization of systems and network resources, advanced and cognitive networking of information objects), need to shape and re-define the overall FI network architecture. To "encounter" such critical challenges, the main goal of Self-NET Project effort is to specify and evaluate new paradigms for the management of complex and heterogeneous network infrastructures and systems (such as cellular, wireless, fixed and IP networks), taking into consideration the next generation Internet environment and the convergence of Internet and mobile networks. Thus, it can efficiently incorporate new operational capabilities in the "*underlying system*" by introducing novel self-management attributes, resulting in significant benefits. Self-NET develops self-management features that alleviate consequences of events for which the system would require various invocations of remedy actions and/or human intervention. This dynamic behavior and intelligence of handling various events (and/or situations) can potentially lead to an innovative and much promising beneficiary scope of the entire system's operations.

Acknowledgments. The present work has been performed in the scope of the *Self-NET* ("*Self-Management of Cognitive Future Internet Elements*") European Research Project and has been supported by the Commission of the European Communities - *Information Society and Media Directorate General* (FP7-GA No.224344).

References

1. Commission of the European Communities. Communication on A public-private partnership on the Future Internet [COM(2009) 479 final, 28.10.2009], Brussels (2009)
2. Castells, M.: The Information Age: Economy, Society, and Culture. Blackwell, Oxford (1996)
3. Commission of the European Communities. Communication on i2010 - A European Information Society for growth and employment [COM(2005) 229 final, 01.06.2005], Brussels, Belgium (2005).
4. Reding, V.: Internet of the future: Europe must be a key player (Speech of February 02, 2009) - Future of the Internet initiative of the Lisbon Council, Commission of the European Communities, DG Information Society and Media, Brussels, Belgium (2009)
5. Chochliouros, I.P., Spiliopoulou, A.S.: Broadband Access in the European Union: An Enabler for Technical Progress, Business Renewal and Social Development. The International Journal of Infonomics (IJI) 1, 5–21 (2005)
6. Timmers, P.: Business Models for Electronic Markets. International Journal on Electronic Markets and Business Media 8(2), 3–8 (1998)
7. Future Internet Assembly (FIA). Position Paper: Real World Internet (2009), `http://rwi.future-internet.eu/index.php/Position_Paper`
8. Afuah, A., Tucci, C.L.: Internet Business Models and Strategies: Text and Cases. McGraw-Hill, New York (2000)
9. Porter, M.E.: Strategy and the Internet. Harvard Business Review 79(3), 63–78 (2001)
10. Commission of the European Communities. Future Internet 2020 - Call for action by a high level visionary panel. Commission of the European Communities, DG Information Society and Media, Brussels, Belgium (May 2009)
11. `http://www.future-internet.eu/`
12. Blumenthal, M.S., Clark, D.D.: Rethinking the design of the Internet: The End-to-End arguments vs. The Brave New World. ACM Transactions on Internet Technology 1(1), 70–109 (2001)
13. Commission of the European Communities. Communication on eEurope 2005: An information society for all [COM(2002) 263 final, 28.05.2002], Brussels, Belgium (2002)
14. Commission of the European Communities. Consultation on the Future EU 2020 Strategy [COM(2009) 647 final, 24.11.2009], Brussels, Belgium (2009)
15. Tselentis, G., Domingue, L., Galis, A., Gavras, A., et al.: Towards the Future Internet - A European Research Perspective. IOS Press, Amsterdam (2009)
16. Chochliouros, I.P., Spiliopoulou, A.S.: European Standardization Activities: An Enabling Factor for the Competitive Development of the Information Society. The Journal of the Communications Network (TCN) 2(1), 62–68 (2003)
17. Organization for Economic Co-operation and Development (OECD). The Seoul Declaration for the Future of the Internet Economy, Paris, France (2008)

18. Chochliouros, I.P., Spiliopoulou, A.S.: Innovative Horizons for Europe: The New European Telecom Framework for the Development of Modern Electronic Networks and Services. The Journal of The Communications Network (TCN) 2(4), 53–62 (2003)
19. Commission of the European Communities. Communication on Future Networks and the Internet [COM(2008) 594 final, 29.09.2008], Brussels, Belgium (2008)
20. Galis, A., Brunner, M., Abramowitz, H.: MANA Position Paper: Management and Service-aware Networking Architectures (MANA) for Future Internets. Draft 5.0 (December 2008)
21. International Telecommunication Union - Telecommunication Standardization Sector (ITU-T). Recommendation M. 3400: TMN Management Functions, Geneva, Switzerland (2000)
22. Pastor-Satorras, R., Vespignani, A.: Evolution and Structure of the Internet: A Statistical Physics Approach. Cambridge University Press, Cambridge (2004)
23. Pastor-Satorras, R., Vásquez, A., Vespignani, A.: Dynamic and Correlation Properties of the Internet. Phys. Rev. Lett. 87(25), 258701–258704 (2001)
24. Faloutsos, M., Faloutsos, P., Faloutsos, C.: On power-law relationships of the Internet topology. In: Proceedings of the Conference on Applications, technologies, architectures and protocols for computer communications, Cambridge, MA, US, pp. 251–262 (1999)
25. Boccalettia, S., Latora, V., Moreno, Y., Chavez, M., Hwang, D.-U.: Complex networks: Structure and dynamics. Elsevier Physics Reports 424, 175–308 (2006)
26. Hegering, H.H., Abeck, S., Neumaier, B.: Integrated management of networked systems: Concepts, architectures, and their operational application. Morgan Kaufmann Series in Networking (1999)
27. `http://www.future-internet.eu/home/future-internet-assembly/stockholm-november-2009/_cross-topic-sessions.html#c199`
28. Réka, A., Barabási, A.-L.: Statistical mechanics of complex networks. Rev. Mod. Phys. 74, 47–97 (2002)
29. Kim, S.-S., Choi, M.-J., Ju, H.-T., Ejiri, M., Won-Ki Hong, J.: Towards Management Requirements of Future Internet. In: Challenges for Next-Generation Network Operations and Service Management, Berlin, Heidelberg, pp. 156–166 (2008)
30. Clark, D., Sollins, K., Wroclawski, J., Katabi, D., Kulik, J., Yang, X.: New Arch: Future Generation Internet Architecture (Final Technical Report) – Issued by the US Air Force Research Laboratory (2003), `http://www.isi.edu/newarch/`
31. Self-NET EU Project, INFSO-ICT-224344, `https://www.ict-selfnet.eu/`
32. Polychronopoulos, C., Kousaridas, A., Alonistioti, N.: Self-Management for Future Internet-Self-NET Project Highlights. Presentation given at the IEEE WCNC 2009- Autonomics for the Future Internet Panel, Budapest, Hungary (April 08, 2009)
33. Chochliouros, I.P., Spiliopoulou, A.S., Georgiadou, E., Belesioti, M., Sfakianakis, E., Agapiou, G., Alonistioti, N.: A Model for Autonomic Network Management in the Scope of the Future Internet. In: Proceedings of the 48th FITCE International Congress, Prague, Czech Republic, pp. 102–106 (September 03-05, 2009)
34. Kousaridas, A., Polychronopoulos, C., Alonistioti, N., Marikar, A., Mödeker, J., Mihailovic, A., Agapiou, G., Chochliouros, I.P., Heliotis, G.: Future Internet Elements: Cognition and Self-Management Design Issues. In: Proceedings of the 2nd International Conference on Autonomic Computing and Communication Systems (SAC-FIRE Workshop), Autonomics 2008, Article No.13, Turin, Italy (September 23-25, 2008)
35. The Netherlands Ministry of Economic Affairs.The Internet: A Shared Future (Publication Number 08ET13). The Hague, the Netherlands Ministry of Economic Affairs (2008)

36. Dobson, S., Denazis, S., Fernandez, A., Gaíti, D., Gelenbe, E., Massacci, F., et al.: A survey of autonomic communications. ACM Transactions on Autonomous and Adaptive Systems (TAAS) 1(2), 223–259 (2006)
37. Mihailovic, A., Chochliouros, I.P., Kousaridas, A., Nguengang, G., et al.: Architectural Principles for Synergy of Self-Management and Future internet Evolutions. In: The Proceedings of the ICT Mobile Summit 2009, Santander, Spain (June 10-12, 2009)
38. Self-NET Project. Deliverable D1.1: System Deployment Scenarios and Use Cases for Cognitive Management of Future Internet Elements (2008)
39. Directorate General Information Society and Media of the European Commission. A Compendium of European Projects on ICT Research Supported by the EU 7th Framework Programme for RTD. Brussels, European Commission (2008)
40. Agoulmine, N., Balasubramaniam, S., Botvitch, D., Strassner, J., Lehtihet, E., Donnelly, W.: Challenges for Autonomic Network Management. In: Proceedings of the 1st IEEE International Workshop on Modelling Autonomic Communications Environments, Dublin, Ireland (October 25-26, 2006), `http://eprints.wit.ie/744/1/MACE2006-final.pdf`
41. Strassner, J.: Autonomic Networking Theory and Practice. IEEE Tutorial (December 2004)
42. Strassner, J.: Policy-Based Network Management. Morgan Kaufmann Publishers, San Francisco (2003)
43. Elliott, C., Heile, B.: Self-organizing, self-healing wireless networks. In: Proceedings of IEEE International Conference on Personal Wireless Communications, pp. 355–362 (December 17-20, 2000)
44. Lewis, L.: Managing Business and Service Networks. Kluwer Academics/Plenum Publishers (2001)
45. Self-NET Project. Deliverable D5.1: First Report on Business Opportunities (2009)
46. Miller, B.: The autonomic computing edge: Can you CHOP up autonomic computing? IBM Corporation (2008), `http://www.ibm.com/developerworks/autonomic/library/ac-edge4/`
47. Prehofer, C., Bettstetter, C.: Self-Organization in Communication Networks: Principles and Design Paradigms. IEEE Communications Magazine 43(7), 78–85 (2005)
48. Gibbens, R.J., Kelly, F.P.: Resource pricing and evolution of congestion control. Automatica 35, 1969–1985 (1999)

Design and Development of Essential Use-Cases for Self-management in Future Internet Wireless Networks

Ioannis P. Chochliouros[1], Evangelos Sfakianakis[1], Apostolis Kousaridas[2],
Jens Modeker[3], David Wagner[3], Anastasia S. Spiliopoulou[4], George Agapiou[1],
Andrej Mihailovic[5], Dev Pramil Audsin[5], Maria Belesioti[1], Andreas Rigas[1],
Konstantinos Chelidonis[1], Evangelos Gazis[2], Gerard Nguengang[6], Nancy Alonistioti[2],
Christos Mizikakis[1], Dimitrios Katsaros[1], and Tilemachos Doukoglou[1]

[1] Hellenic Telecommunications Organization (O.T.E.) S.A.,
Research Programs Section, Labs & New Technologies Division,
Pelika & Spartis Street, 15122 Maroussi, Athens, Greece
{ichochliouros,esfak,gagapiou,mbelesioti,arigas,khelidon,
xmizikakis,dimkatsar,tdouk}@oteresearch.gr
[2] Dept. of Informatics and Communications, University of Athens,
15784, Panepistimioupolis, Ilissia, Athens, Greece
{akousar,gazis,nancy}@di.uoa.gr
[3] Fraunhofer FOKUS, Competence Center Network Research, Sankt Augustin, Germany
{Jens.Modeker,David.Wagner}@fokus.fraunhofer.de
[4] Hellenic Telecommunications Organization (O.T.E.) S.A.,
General Directorate for Regulatory Affairs,
99, Kifissias Avenue, 15124 Maroussi, Athens, Greece
aspiliopoul@ote.gr
[5] King's College London (KCL)
Centre for Telecommunications Research, London, UK
{andrej.mihailovic,Dev.audsin}@kcl.ac.uk
[6] Thales Communications France
Gerard.nguengang@thalesgroup.com

Abstract. The paper discusses and describes several selected use-cases for autonomic/cognitive management purposes in the scope of the Future Internet (FI) evolution, as these have been identified upon the original context of the EU-funded Self-NET Project effort. The essential aim is to "delimit" new paradigms for the management of complex and heterogeneous wireless network infrastructures and systems, by proposing the operation of self-managed FI elements around a novel feedback-control cycle, known as the MDE cognitive cycle. Thus, the paper intends to "identify" an integrated validation environment for the prototyping and the assessment of relevant concepts and artifacts, via the establishment of appropriate use-cases and corresponding scenarios of use and the explicit description/set-up of relevant test-beds and/or implementation platforms, towards network and node management. The three proposed use-cases have been selected as "proper drivers" for the design and the validation of Self-NET architecture and concepts.

Keywords: Autonomic communications, cognitive networks, Future Internet, generic cognitive cycle model, mobility management, network capacity optimization

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 318–333, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

routing adaptation, self-configuration, self-management, routing adaptation, traffic management, wireless access network coverage.

1 Introduction

The Internet world as we know it today has undergone far reaching changes since its early days while becoming a critical communications infrastructure underpinning our economic performance and social welfare. Rapid technological and social changes, together with the bewildering emergence of numerous new services and the increasing number and complexity of access technologies have created a complex environment for network operators/service providers and a challenging situation for end-users [1]. The enhancement of existing information and communication technologies (ICT) and the development of new systems will even further increase this complexity. The Internet architecture and its protocols are currently the targeted technology for future operator business [2]. As the Internet has actually moved from a research curiosity to a recognized component of mainstream society [3], new requirements are continuously emerging and they implicate completely new design principles.

According to the international practice, in a re-design of the current communication environment, a number of requirements have to be considered to have an excellently running and easy to manage system: (a) Security, by also taking into account end-user satisfaction through hidden transmission and safeness of the communication equipment, in order to ensure that the network is sufficiently protected from unauthorized users; (b) Reliability (i.e. protection from network interrupts) and making sure the network is available to users and responding to hardware and software malfunctions; (c) Network management and self configuration ability, i.e. automatic provisioning of services and dynamic adaptations of resource requests; (d) Self-healing ability, i.e. automatic identification of sources of failures and reconfiguration of the network; (e) Scalability, for an efficient management of millions of end-users, network devices, sensors and their networks; (f) Quality of Service (e.g. delay, jitter, bandwidth) and Quality of Experience (end-to-end QoS), and; (g) Support of mobility feature (inter-technology, intra-technology, inter-operator domain, and intra-operator domain), when possible. The current Internet plane environment is complex and not always capable to provide such services in an easy way. Therefore, fundamental new techniques have to be invented to decrease the complexity and to exploit all potential benefits [4], thus creating a fully innovative "*complex*" entity (including network and facilities-services). Research initiatives are being created directed on Future Internet (FI) evolutions and many approaches have been analysed and challenges for evolution have been presented [5], [6]. In this context are performed the targeted activities of the Self-NET Project effort [7], aiming to specify and evaluate new paradigms for the management of complex and heterogeneous network infrastructures and systems, such as cellular, wireless, fixed and IP networks, and taking into consideration the next generation Internet environment and the convergence of Internet and mobile networks. The essential idea is "*to bring more intelligence*" at the network element level in order to enable the network to "*self-pilot its behaviour*" within the constraints of high level business goals. With Self-NET nodes, administrators will focus more on the definition of high levels constraints and less on root cause analysis and low level devices configuration process; the management process will be simplify by automating and distributing the decision-making process involved in the network operation optimization. Powerful management capabilities will be embedded in the network elements thanks to an innovative feedback control cycle, i.e. the *"Monitoring, Decision-Making and Execution (MDE) cognitive cycle*". The MDE cycle will enhance the network element (NE) functionalities by allowing each network device to understand what is happening in its environment, deduce from this understanding the relevant set of actions required to solve the encountered abnormal situation within the constraints of business goals and enforce the corresponding configuration to recover from the anomaly [8].

Self-NET system architecture aims to incorporate the innovative aspects related to the related specific Future Internet topics, i.e., autonomic networking, network management, knowledge management, self-configuration and optimisation, and native Internet themes. In order to design the Future Internet network elements, Self-NET has identified several scenarios and thirteen use-cases have been defined [9]. Based on these use-cases, the Project has extracted FI functional requirements and has designed a knowledge framework that introduces cognitive capabilities at various level of the network ranging from the network element level to the domain level. Dynamic and flexible forwarding mechanisms have been designed to allow more adaptability of the protocols stack [10]. Based on the addressed technical areas, the relevance with respect to the work achieved in the wider Self-NET context and the availability of involved equipments, the Project has selected the following four use-cases as the "drivers" for testing and validation activities: (a) Coverage and capacity organization in wireless environments; (b) Traffic management, re-routing and forwarding to support mobility, QoS and routing adaptation, (c) Dynamic spectrum re-allocation for efficient use of traffic, and; (d) Adaptable routing and mobility management in dynamic self-managed wireless mesh topologies.

The paper provides a description of the selected three use-cases, as the latter have been proposed by several Self-NET partners. A strong emphasis is made on the integration of the knowledge framework that implements all the aspects of the MDE cycle. For each separate use-case we consider a brief description providing clarifications and/or informative data about: the background of the specific use-case; the detailed description of the corresponding test-bed and the role of each segment; the monitoring protocols that will be used to retrieve information from network elements; testing and validation perspectives, and; finally a briefing of the introduced innovative features.

2 Description of Use-Case 1: Coverage and Capacity Optimization in Modern Wireless Networking Environments

In current practice, wireless network planning is a difficult and challenging task that involves expert knowledge and profound understanding of the factors affecting and determining the performance of the wireless system. Several monitoring parameters should be taken into account for the optimal coverage and capacity formation, while different configuration actions are available that in many cases are interrelated, as regards the consequences. In established approaches, frequency planning is conducted as part of the deployment procedure for entire network segments or domains.

The assignment of operating frequencies and/or channels to wireless network elements is also a part of the frequency planning procedure. To eliminate conflicts in frequency assignment, the procedure is centrally coordinated in a procedure that assumes and requires global knowledge and control over the concerned network segment or domain. In this context, global knowledge and control implies that the administrative entities are fully aware of the channel assigned to each individual network element and are fully capable of adjusting such assignments to their liking in a centrally coordinated manner. As a result, conflicts in frequency assignment may be avoided or, *at least*, minimized, provided that a central entity coordinates the entire procedure. Apart from the optimal channel allocation, the load balancing and the distribution of the users to the available access points, in the context of a multi-RAT (Radio Access Terminal) environment is an another key issue for next generation communication networks that will be studied through this use-case. In a large-scale distributed setting, where multiple independent stakeholders operate one or more network infrastructures offering wireless access, central planning and control are neither realistic, nor "feasible" options. The independence of each stakeholder suggests that peer approaches are more suitable in this setting, either in a cooperative or a non-cooperative manner. Hence, a technical approach based on the locally available state information and the interaction with peers through explicit or implicit approaches is favored in this setting.

Existing standards for popular wireless access technologies do not provide the capacity to interact with peers on the basis of local and exchanged information for purposes of improving coverage and capacity [11]. Each wireless access system or network segment comprising multiple access systems is configured independently of all others. As a result, in cases where technical expertise falls short of the complexity involved in efficient frequency planning for an infrastructure free -or at least one with a controlled level- intra-band and inter-band interference, system performance is seriously degraded due to inefficient channel assignment. Addressing this problem on the basis of coordination among different administrations may work only for large scale installations where network management personnel is skilled in solving frequency planning problems through a set of established procedures. This is the case for cellular network operators where frequency bands are typically allocated for prolonged time periods (i.e., decades) according to some form of auction. In these settings, radio network planning is a well-structured process that leverages skilled technicians to ensure the most efficient use of the expensive spectrum resource.

However, in the huge mass consumer market segment targeted by modern WLAN (Wide Local Area Network) technologies this approach is not realistically feasible, for a number of reasons. First and foremost, the typical consumer does not possess the technical expertise required to fully comprehend and efficiently solve such frequency planning problems. Even if that was the case, achieving an efficient coordination among a large number of consumers where each controls a single wireless access system (e.g., a residential broadband gateway with an embedded WLAN access point) would be extremely difficult.

Therefore, the introduction of an autonomic mechanism that undertakes the discovery of conflicting frequency plans in-situ and initiates reactive measures to adapt frequency and/or channel assignments in a collaborative manner among the concerned network elements is necessary. In addition to being purely reactive in nature, such a mechanism may also possess additional intelligence that enables it to record adaptation decisions and correlate them to temporally collocated observations regarding the context in which those observations were made. These correlations are to be exploited in the future as part of and to improve the decision making process for similar adaptation situations [12].

The scenario considered assumes access network segments with Wireless LANs. The target problems are perceived as follows: Resource (Channel) allocation conflicts causing primarily poor resource (spectrum band) utilization and, as a consequence, delay in medium access, congestion due to inference limiting channel throughput, inability to support QoS-sensitive and real-time applications efficiently and, at a wider scope, increased capacity requirements. No protocol or standard is available and operator's intervention is necessary. In particular, if considering the network topology that is described in Fig.1, four phases have been considered for the scenario description and thus the demonstration of the developed mechanisms: (i) Activation of an access point at an already established network topology and demonstration of the self-configuration process; (ii) De-activation of an access point and network topology self-organization; (iii) Self-Optimization of the network topology due to the identification of a fault, demonstrating thus the full aspects of the decision making module, and; (iv) Improvement of the deduction and decision making mechanisms, exploiting the available feedback loops. For the actual use-case, two specific test-bed facilities have been taken into account (as discussed in the following sub-clauses 2.1 and 2.2) and are integrated in order to increase the configuration capabilities and enrich the situations that the Self-NET cognitive plane may address.

2.1 Description of Test-Bed 1 (Proposed by the University of Athens-UoA)

The essential structure of the first test-bed that is also depicted in Fig.1 is analyzed, briefly, as follows:

- *Infrastructure:* A WLAN access network segment with Network Address Translation (NAT) access to Internet and port forwarding for specific services.
- *Involved technologies:* IEEE 802.11b/g, static routing tables in the access network segment (no routing protocol in effect), and SNMP (Simple Network Management Protocol). For the realization of the "added" intelligence and cognition of the NECMs/NDCMs (Network Element Cognitive Managers/Network Domain Cognitive Managers) in the network nodes (i.e. Soekris devices [13]) and, more specifically for the decision making part, the fuzzy logic technique has been used for the inferences as well as specified objective functions for the channel allocation problem. Furthermore, neural networks and the K-Means methods have been utilised for the identification of patterns for network observations as well as for the feedback/learning process.
- *Monitoring tools:* All SNMP primitives using the SNMP protocol (port forwarded over the NAT), SSH (secure shell) remote command execution. SNMP (which is used as *monitoring protocol*) is intended to used locally as a standardized monitoring protocol (local monitoring actions), by the NECMs without the existence of a central SNMP manager that collects and re-distributes the monitoring data. A CACTI [14] installation mainly used for visualization purposes, exists in the WLAN network segment for local monitoring purposes using a dedicated network segment.

- Proposed *monitored parameters* are: Link quality, Signal level, Noise level, Rx invalid nwid, Rx invalid crypt, Rx invalid frag, Invalid misc, Channels occupied.
- *Prerequisites:* Ability to place the MiniPCI WLAN card on the Soekris boards on master mode so as to support the software-based access point daemon.
- *Initial conditions:* Soekris access points using a channel allocation pattern with at least one conflict. In fact, this requirement stems from the scenario in question.
- *Assumptions and constraints:* Local NECMs should be able to communicate directly; thus a 2nd wired interface is used for the exchange of control information.

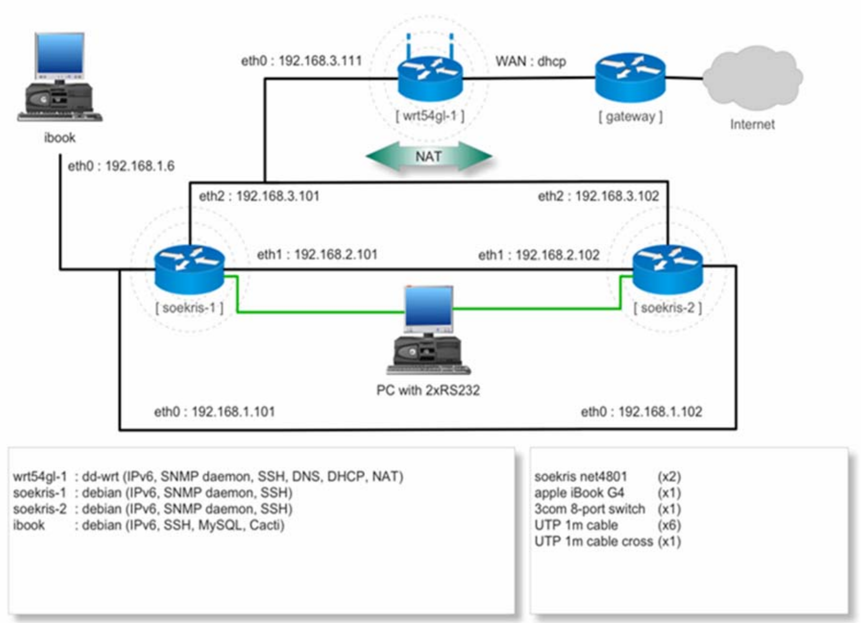


Fig. 1. Use-case 1: Topology of the *University of Athens* Test-bed

Experimental setup:

- *Fault or network anomaly generation:* Interference is caused by spectrum overlap in WLAN defined channels. This may involve only a minimal level of interference, which, however, is detected by proximal WLAN access points and thus serves as a trigger for the induction of processes in the MDE cycle. Optionally, traffic generators may be employed to induce traffic over the Soekris access points and, *thus*, heavy interference in selected WLAN channels.
- *Anomaly detection:* Primarily, a mathematical formula is used to assess metrics related to channel overlap based on specific variables retrieved over the SNMP and/or SSH protocols and concerning “key WLAN parameters” (e.g., channel in use, mode in use, transmission power, etc).
- *Configuration protocols and parameters:* The SNMP and/or SSH protocols support configuration, along with static configuration in non-volatile local storage.

2.2 Description of Test-Bed 2 (Proposed by the Hellenic Telecommunications Organization S.A.-OTE)

The proposed test-bed considers a laboratory setting, where a WiMAX base station (BS) resides, operating at 3.5GHz and serves the surrounding area. A potential example concerning the operation of the test-bed may arise if we also consider a small campus nearby the lab premises where, *during some experiments*, a young researcher unaware of all the lab settings, approaches the BS very closely with his laptop, and starts to cause a lot of interference, forcing the BS to start scanning for a another channel. Then a potential operation of the cognitive plane (based on the description previously discussed in the clause 2 of the present work) can be as follows: The situation, due to the interference caused, is also reported to NDCM and after some scanning, the NDCM aware that there are no similar BSs operating nearby, orders the BS to "change" frequency [16]. The essential "drawback" lies upon the fact that even though the band is licensed, interference deteriorates system performance, resulting in reduced channel throughput, limited support of QoS and delay sensitive applications. Therefore, causing increased capacity demand. The proposed approach implicates that a proper radio planning is required, which is mostly static and its handling also requires human management. Interference is measured in various channels and another one is selected for use in the cell/sector. Then both the CPEs (Customer Premises Equipment) and BS move to the selected frequency with less interference. In case of

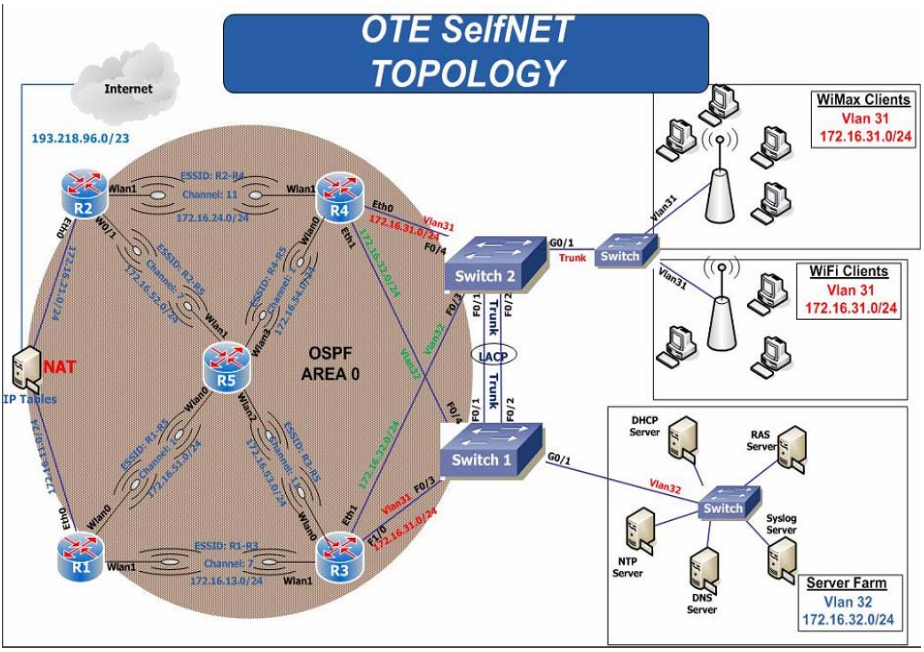


Fig. 2. Use-case 1: Topology of the *OTE (Hellenic Telecoms Organization SA)* Test-bed

increased interference (e.g. low Signal-to-Noise ratio, SNR), the NDCM will be responsible for changing the frequencies of both the BS and the Subscriber Unit (CPE). Additionally, when NDCM detects high Signal-to-Noise ratios for all subscribers and hence good transmission environment, the long cyclic prefix used in multipath environments could be changed to short cyclic prefix, improving thus the total throughput of the system.

The essential structure of the second test-bed (as illustrated in Fig.2) is as follows:

- *Infrastructure:* WiMAX network segment interconnected with Ethernet infrastructure consisting of Cisco and Linux-PCs, operating as switches and routers, providing also a few virtual LANs. Access to Internet is provided through NAT. Another wireless segment using Wi-Fi, which is operating at 2.4 GHz, is connected to the core network.
- *Involved technologies:* IEEE 802.16d, OSPF (Open Shortest Path First) is used in the routers and LACP (Link Aggregation Control Protocol) and STP (Simple Transfer Protocol) by the switches, SNMP for management purposes; SSH remote command execution; DNS (Domain Name System), DHCP (Dynamic Host Configuration protocol), NTP (Network Time Protocol) services running in the network.
- *Monitoring protocol:* SNMP.
- *Routing/Switching protocols*: OSPF (L3), LACP and STP (L2).
- *Monitored parameters (at the 802.16 segment):* SNR, Signal Modulation, CRC (Cyclic Redundancy Check) Errors, Channels occupied.
- *Monitoring Tool:* Redline Monitoring Tool in the WLAN network segment for local monitoring. SNMP, IPtables, SNORT, Syslog for all monitoring purposes.
- *Prerequisites:* Ability to connect Redline BS with a PC hosting the software-based access point daemon (hostapd). The daemon needs to support SNMP commands for the Redline BS management. Necessary sensors and other NEs are to be placed throughout the network.
- *Initial conditions:* Redline WiMAX Base Station (IEEE 802.16d) with an initial channel allocation pattern, according to the corresponding scenario's description.
- *Assumptions and constraints:* NEs issue commands understandable by the underlying network equipment (i.e., in particular from the Redline BS and the Cisco switches and routers). Since most of the network equipment is proprietary, it provides limited configurability in certain aspects and especially in real time changes of configuration. Additionally, there will be a (possible direct) connection maintained between the NDCM, NEs for the communication between them.

Activities of the cognitive framework integration under the consideration of the MDE approach:

- *Monitoring:* Monitoring is supported by the SNMP daemon on the Soekris systems (IEEE 802.11) as well as on the WiMAX BS (IEEE 802.16d) and complemented by the capacity to execute any operating system command over the SSH protocol and intelligently parse the command's output, *if necessary*. Furthermore, monitored data may also be collected and concentrated by a dedicated software established on an involved network element e.g., a network element that hosts Nagios.

- *Situation Awareness (SA):* It is supported as part of, and within the cognitive management framework instrumentation, where a loosely coupled mode of interaction is based on events and subscription to event topics of interest.
- *Decision Making:* Initially, the Fuzzy logic algorithms and utility functions have been selected for the first part of the corresponding use-case. Both placed at the decision making engine of the NECM and the NDCM.
- *Learning:* Supervised and Semi-supervised machine learning approaches (e.g., neural networks, k-means) are initially studied and developed using also WEKA libraries [15] for the off-line improvement of the decision making process.
- *Execution:* It is supported by the SNMP daemon on the Soekris systems and is "identical" to the relevant *Monitoring* activity. Similarly the SNMP daemon of the Redline WiMAX BS systems is used for the configuration actions that are issued by the NECM or the NDCM towards the WiMAX subsystem.

The target functionalities arising from the scope of the use-case 1 are summarized as follows:

- *Dynamic optimization capability through local NECMs collaboration and NDCMs hints/recommendations:* The system "*optimizes itself*" in case of a sub-optimal channel allocation while considering wireless link status and conditions.
- *Dynamic auto-configuration capability:* The system detects a significant change in its operational context (e.g., the introduction of additional network elements requiring access to the wireless resource). In response to this event, it undertakes the configuration of the proper resource assignment plan to accommodate both existing and new NEs. In particular, planning involves the assignment of a wireless channel and, optionally, the adjustment of radio transmission parameters.

The main innovations of the above contextual "approach" are listed as follows: (i) *Automation:* Compute/perform reconfiguration solutions to solve context problems; (ii) *Detection of problematic situation:* The system autonomously monitors aspects of its operational context and detects significant deviations from the set of states that determine "optimum" or "optimal" performance; (iii) *Optimization based on local interactions:* The system approaches or reaches an optimum mode of operation by exploiting local state and information exchange with peers. A scoping mechanism confines signalling and avoids scaling problems; (iv) *Self-optimization* in case of sub-optimal resource assignment or performance; (v) *Adaptability capabilities* in the face of unknown network topology and wireless conditions, and; (vi) *Distribution of decision mechanisms* by involving local/global interaction at the level of information management and dissemination.

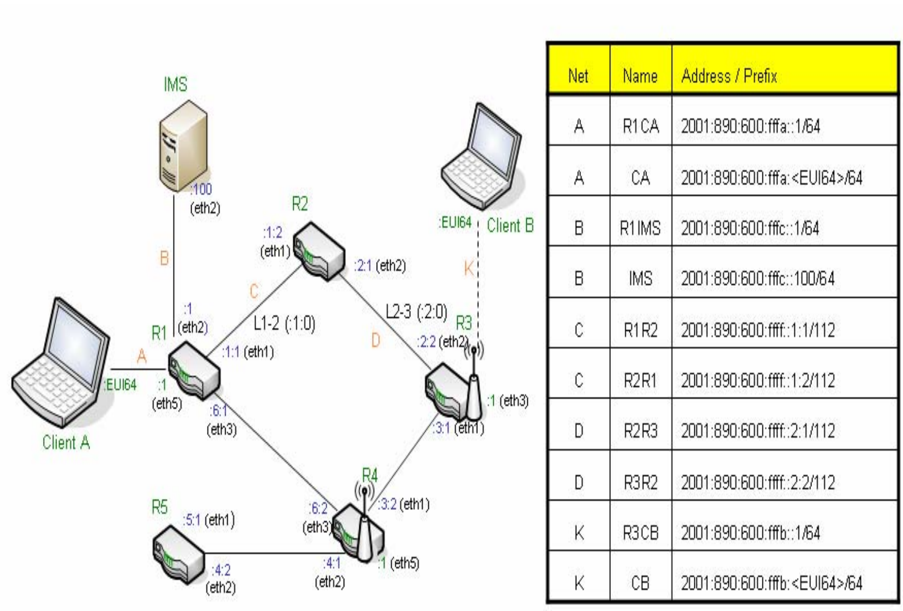
3 Description of Use-Case 2: Traffic Management, Re-Routing and Forwarding to Support Mobility, QoS and Routing Adaptation

When packet loss occurs, today's network management cannot always provide multiple options: it is possible to "change" routes and/or the deployment of nodes may be changed as a whole, but this is normally quite expensive and therefore it is usually avoided. When this comes to be the case in wireless networks (also including wireless backhauls), it would be appropriate to have the ability to "*modify*" several link characteristics like modulation, FEC (Forward Error Correction) or retransmissions on-the-fly and maybe temporary only. This would allow "tailoring" the wireless network to the "*normal case*" rather than the "*worst case*" and the use of cheaper (e.g. WiFi-based) equipment. This is an area where the capability to "*dynamically*" adopt network functionality could be extremely beneficiary, for the entire network behavior. The present use-case targets packet loss avoidance for a wireless link and incorporates the control of the DPC (Dynamic Protocol Composition) framework – the latter is a novel execution capability. The NECM derives that the monitored packet loss is due to bad link quality and decides to activate on its own ARQ (Automatic Repeat Request) to the next Self-NET node using Functional Protocol Elements (FPEs) in the DPC framework.

This affects part of the path of a video streaming flow which in return will improve significantly. The relevant test-bed is depicted in Fig.3. The use-case targets general network performance improvement by the means of activation of FPEs. It includes several possible adaptations for controlling traffic, e.g. diverting traffic or changing functionality like ARQ for flows of packets. Focus in the execution part of this use-case is the usage of functionality composed by several FPEs which may establish or change specific functions in the network e.g. changing a route or adding a protocol function like ARQ. Since the set of potential options and combinations is huge, the case is restricted to two triggers, namely an overloaded node and losses on a specific link. Current protocols and networks provide means neither to the receiver nor the sender to handle or alleviate such situations. In Fig.3 we illustrate the topology of the relevant test-bed.

Test-bed description (proposed by Fraunhofer Fokus):

- *Involved technologies:* The test-bed consists of the core routers (5PCs with Ubuntu 8.10 server), the Open IMS (IP Multimedia Subsystem) Core [17] (1 Ubuntu 8.10 server), the WLAN access point and two Clients (Linphone, SIP Communicator, or Monster).
- *Infrastructure:* Open IMS Core reconfigured to enable IPv6, Router advertisement daemon (radvd) [18] sending periodically Router Solicitation message which is required for IPv6 stateless auto-configuration (installed on R1, R3 and R4), Netem [19] (emulates variable delay, loss, duplication and re-ordering), Iperf (network testing tool that can create TCP (transmission control protocol) and UDP (user datagram protocol) data streams and measure the throughput of the network [20]), Ipv4 for management purposes.
- *Monitoring tools:* bwm-ng (Bandwidth Monitor NG) [21] installed on all routers, Network protocol Analyser TShark [22] installed on the Open IMS Core and on the layer 3 components. (There are no *monitoring protocols*).
- *Monitored parameters:* Bandwidth, load and loss detection on all nodes.
- *Prerequisites:* Clients registered at the OPEN IMS Core.
- *Initial conditions:* A SIP (Session Initiation Protocol) session is established and video is being streamed from A to B.



Net	Name	Address / Prefix
A	R1CA	2001:890:600:fffa::1/64
A	CA	2001:890:600:fffa:<EUI64>/64
B	R1IMS	2001:890:600:fffc::1/64
B	IMS	2001:890:600:fffc::100/64
C	R1R2	2001:890:600:ffff::1:1/112
C	R2R1	2001:890:600:ffff::1:2/112
D	R2R3	2001:890:600:ffff::2:1/112
D	R3R2	2001:890:600:ffff::2:2/112
K	R3CB	2001:890:600:fffb::1/64
K	CB	2001:890:600:fffb:<EUI64>/64

Fig. 3. Use-case 2: Topology of the *Fraunhofer Fokus* Test-bed

- *Assumptions and constraints:* The ability to implement the FPEs and the protocol function (e.g. ARQ) into routers. Furthermore to label the RTP (Real-Time Transport Protocol) packages and to change the routing table entries.

Experimental setup:

- *Fault or network anomaly generation:* Interference is caused by Netem (emulates variable delay, loss, duplication & re-ordering) and Iperf/Multi-Generator (MGEN) [23] (generates overload).
- *Anomaly detection:* Threshold based and statistical analysis of current throughput, packet loss and also correlation of multiple inputs including static information (like max. bandwidth), technology.
- *Configuration protocols and parameters:* SSH protocol support configuration.

Activities under the consideration of the MDE approach:

- *Monitoring* of packet loss is performed by reading retransmission using tshark.
- *Decision Making:* Using the monitored data together with a certain threshold will be utilized to derive decision making techniques.
- *Execution:* Reconfiguration of the DPC framework by enabling Link Local ARQ.

The introduced use-case can demonstrate the benefits of in-network protocol functionality that can be dynamically (and transparently) reconfigured by cognitive network management activities.

The main innovations of the proposed consideration are given, in brief, as follows: (i) *Enabling the network to interpret flow specifics*, by the provision of generalised Information Elements; (ii) *Recognition/identification* of “where packet loss has happened in the network, and compute appropriate reaction by enabling ARQ at network segment; (iii) *Introduction of fine-grained protocol functionality* to the network nodes that do not act as end-nodes, and; (iv) Unlo*ad of the network* by reducing the amount of retransmissions traffic, by rather focusing retransmissions at the hop where the packet losses are caused.

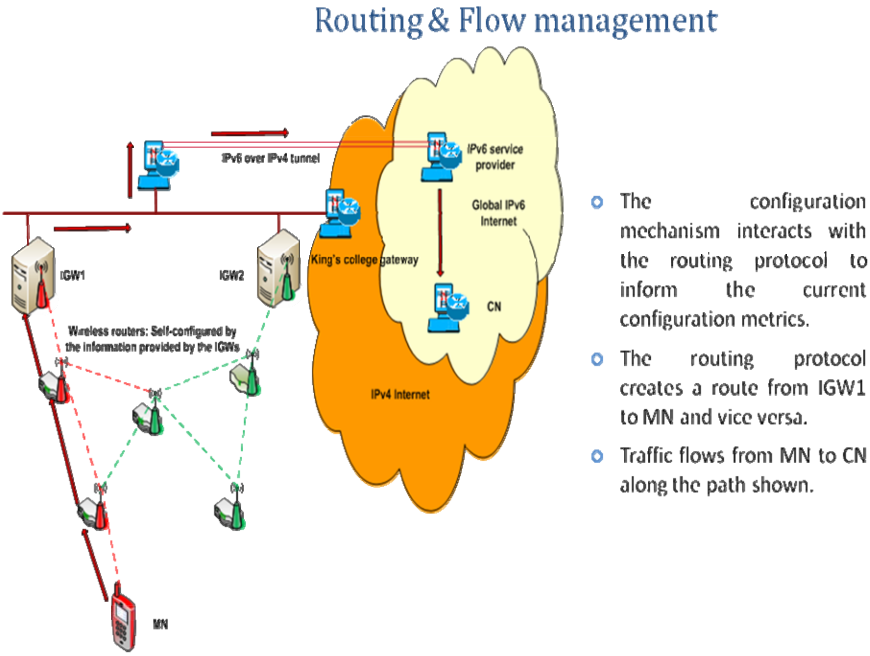
4 Description of Use-Case 3: Adaptable Routing and Mobility Management in Dynamic Self-managed Wireless Mesh Topologies

This use-case provides a mechanism for the provision of network connectivity, handover and flow re-directions for mesh networks. This use-case provides a path for the intelligent network elements by implementing some of the characteristics of self-management. The scenario concentrates on the self-X methods for the provision of the Internet, by establishing mechanisms for the NEs in order: to configure themselves with optimal information; to monitor the network dynamics, and; to adapt themselves by re-configuring the needed information. This will result in the changes to the mobile node’s configuration making the mobile node to do a handover. On the other hand, NEs’ re-configuration to maintain optimal configuration affects the routing protocol configuration and the operations leading to the re-direction of the packet flows.

The developed protocols in action will function during the initial bootstrapping phase as well as re-configuration phase of the NEs. The target problem areas include dynamic configuration of NEs with optimal metrics taking into account of network dynamics, such as deployment of additional nodes, network element failure, topology changes and mobility resulting in the re-direction of traffic flows. Fig.4 illustrates the topology of the relevant test-bed.

Test bed description (proposed by the King’s College London-KCL)

- *Infrastructure:* WLAN, access networks, wired LANs, mesh (or “*mesh-like*”) networks, with ability to connect to global IPv6 Internet.
- *Involved technologies:* IEEE 802.11 b/g, Link state routing protocol, SNMP, self-configuration and mobility management.
- *Monitoring tools:* POSIX system functions, Linux primitives.
- *Monitored entities:* Link state and characteristics, network interface, routing protocol and IPv6 configuration elements.
- *Prerequisites:* Ability to re-compile the Linux kernel, development and debugging libraries / tools, WLAN card drivers support for de-centralized communication.
- *Initial conditions:* The initial condition arises from the proposed scenario and the requirement for Internet’s provision that is adaptable to the network dynamics with optimal configuration and mobility with ease and minimal network planning and human intervention.



Routing & Flow management

- The configuration mechanism interacts with the routing protocol to inform the current configuration metrics.
- The routing protocol creates a route from IGW1 to MN and vice versa.
- Traffic flows from MN to CN along the path shown.

Fig. 4. Use-case 3: Topology of the *King's College of London-KCL* Test-bed

Experimental setup:

- *Fault or network anomaly generation:* Network induced changes to optimal configuration caused by network topology variations and the NE's dynamics.
- *Anomaly detection:* A self-aware mechanism is used to determine the deviation from optimal configuration. NEs maintain an information base, supporting their configuration mechanism. The configuration methodology should select an optimal configuration for the specified performance metric and is based on a function. The decision is made considering the current configuration, set of available upstream routers, gateway preference. The optimal configuration process is triggered by a NE under two circumstances, namely the bootstrap state and changes to network conditions or, in general, the dynamics of the network environment. In the latter case, the NE should re-configure to provide optimal configuration for the Internet connectivity and traffic flows. NE failure or addition of a NE is a representative example that triggers a network dynamics and eventually changes to the configuration of the NEs. Since, the above mentioned events introduce network dynamics, a gateway with better Internet connectivity is necessary. Each NE, after the trigger for configuration selection or update selects an optimal configuration. The network area or environment for a NE includes all the routers up to the Internet gateway.
- *Configuration protocols and parameters:* SSH protocols to execute operating system and user-defined protocols, applications/commands over the network.

- A description of the mechanisms involved in that directs the monitor the information and the methods that describe the re-configuration are described in Fig.4, where the configuration mechanism interacts with the routing protocol to inform the optimal configuration metrics.

Activities under the consideration of the MDE approach:
The integration of the cognitive manager requires the input such as the address of the Internet gateway, routers and the preference of the configuration element for the decision making process which results in the selection of the optimal configuration, i.e.: routing adaptations, handover of the mobile node and flow re-directions. The action component performs the re-configuration of the NE with optimal configuration, routing protocol adaptations, handover functionality and routing re-directions enhances device's capability.

- *Monitoring* is performed by POSIX system functions, SNMP. The self-management of the network system is achieved by monitoring the network elements such as the routers, mobile node, packet flow paths and redirections and Internet gateway. The monitoring system includes configuration information, traffic flow context, cumulative traffic flow directions and state, collective packet flow information in the network.
- *Decision Making:* The monitored configuration data or parameter is utilized to "derive" decision making techniques, methodologies and processes. This is a functionality of collective analysis and involves methods and functions for the "optimum" decision making and evaluation criteria applied. One relevant process is when a configuration element is to be selected from a set of possible/candidate configuration elements as the most appropriate configuration choice. Another process involves packet redirections constrained with regards to routing and handover mechanisms.
- *Execution:* Execution is supported by Linux system calls, SSH remote execution and SNMP primitives. This implicates optimal initial configuration and re-configuration of network elements, handover trigger, routing protocol re-configuration and adaptations, route table flush and re-establishment, route recalculations, and traffic flow path alterations for handover support.

The target functionalities arising from the scope of this use-case are as follows:

- *Hot reconfiguration of network elements* including routers and mobile nodes with optimal configuration and the *capability to react in case of NE failures*, including the *addition of new NE.*
- *Routing protocol can "adapt" itself to the new configure* and calculates path with respect to the new configuration; this results in the traffic re-routing.

The main innovative features are summarized as follows: (i) Dynamic optimal configuration of network elements with regards to network dynamics; (ii) Routing protocol adaptations and traffic re-routing; (iii) Distributed decision making mechanisms, and; (iv) Decision procedure into multiple levels (NECM, NDCM, etc).

5 Conclusion

The main objective of Self-NET Project is to design and validate new paradigms for the management of complex and heterogeneous network infrastructures and systems, by taking into consideration the next generation Internet environment and the convergence of Internet and mobile networks. Self-NET aims to "engineer" the FI, based on cognitive behavior with a high degree of autonomy, by proposing the operation of self-managed FI elements around a novel feedback-control cycle, the MDE cognitive cycle. This paper aims to provide an integrated validation environment for the prototyping and the assessment of relevant concepts and artefacts, via the establishment of appropriate use-cases and the detailed set-up of relevant test-beds and/or implementation platforms towards efficient network and node management, when anomalies are detected. The paper addresses the issue of scenarios' refinements by providing a detailed description of three use-cases (i.e.: (i) wireless access networks coverage and capacity optimization; (ii) traffic management, re-routing and forwarding to support mobility, QoS and routing adaptation, and; (iii) adaptable routing and mobility management in dynamic self-managed wireless mesh topologies), that have all been selected as essential "drivers" for the validation of Self-NET architecture and concepts.

Acknowledgments. The present work has been performed in the scope of the *Self-NET* ("*Self-Management of Cognitive Future Internet Elements*") European Research Project and has been supported by the Commission of the European Communities - *Information Society and Media Directorate General* (FP7, Grant Agreement No.224344).

References

1. Herring, R.: The Future of the Internet: In a Decade, the Net Will Dig Deeper into Our Lives (April 2006) `http://www.redherring.com/Article.aspx?a=16391&amp;hed=The+Future+of+the+Internet`
2. Clark, C.D., Wroclawski, J., Sollins, K., Braden, R.: Tussle in Cyberspace: Defining Tomorrow's Internet. IEEE/ACM Transactions on Networking 13(3), 582–595 (2005)
3. Afuah, A., Tucci, C.L.: Internet Business Models and Strategies: Text and Cases. McGraw-Hill, New York (2000)
4. European Commission, Information Society and Media: The Future of the Internet: A Compendium of European Projects on ICT Research Supported by the EU 7th Framework Programme for RTD (2008)
5. European Future Internet Portal, `http://future-internet.eu`
6. Future Internet Research and Experimentation, `http://www.ict-fireworks.eu`
7. Self-NET EU Project, INFSO-ICT-224344, `https://www.ict-selfnet.eu/`
8. Chochliouros, I.P., Spiliopoulou, A.S., Georgiadou, E., Belesioti, M., Sfakianakis, E., Agapiou, G., Alonistioti, N.: A Model for Autonomic Network Management in the Scope of the Future Internet. In: Proceedings of the 48th FITCE (Federation of Telecommunications Engineers of the European Union) International Congress ICT Transformation - Global InfoSociety Realization in 2009?, Prague, Czech Republic, pp.102–106 (September 03-05, 2009)

9. Mihailovic, A., Chochliouros, I.P., Kousaridas, A., Nguengang, G., Polychronopoulos, C., Borgel, J., Israel, M., Conan, V., Belesioti, M., Sfakianakis, E., Agapiou, G., Aghvami, H., Alonistioti, N.: Architectural Principles for Synergy of Self-Management and Future internet Evolutions. In: Proceedings of the ICT Mobile Summit 2009, Santander, Spain (June 10-12, 2009)
10. Self-NET Project, Deliverable D1.1: System Deployment Scenarios and Use Cases for Cognitive Management of Future Internet Elements (October 2008), `http://www.ict-selfnet.eu/`
11. DaSilva, M., Ferreira de Rezende, J.: A Dynamic Channel Allocation Mechanism for IEEE 802.11 Networks. In: Proceedings of the VI International Telecommunications Symposium (ITS) Fortaleza-Ce, Brazil, pp. 225–230 (September 03-06, 2006)
12. Akella, A., Judd, G., Seshan, S., Steenkiste, P.: Self-management in chaotic wireless deployments. In: Proceedings of the 11th Annual International Conference on Mobile Computing and Networking (MobiCom 2005), Cologne, Germany, August 28 - September 02, pp. 185–199 (2005)
13. SOEKRIS, `http://www.soekris.com/index.htm`
14. CACTI, `http://www.cacti.net`
15. WEKA, `http://www.cs.waikato.ac.nz/ml/weka`
16. Chochliouros, I.P., Diakonikolaou, G., Belesioti, M., Sfakianakis, E., Spiliopoulou, A.S., Alonistioti, N.: Dynamic Spectrum Reallocation via Autonomic Management. In: Proceedings of the 10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Kos, Greece (June 15-19, 2009)
17. Open IMS Core, `http://www.openimscore.org`
18. Radvd, `http://www.litech.org/radvd`
19. Netem, `http://www.linuxfoundation.org/collaborate/workgroups/networking/netem`
20. Iperf, `http://en.wikipedia.org/wiki/iperf`
21. Bwm-ng, `http://www.groop.org/?id=projects&sub=bwm-ng`
22. TShark, `http://www.wireshark.org/docs/man-pages/tshark.html`
23. MGEN, `http://cs.itd.nrl.navy.mil/work/mgen/7`

Towards Dynamic Protocol Configuration and its Configuration and Control in Autonomous Communication Environments

David Wagner and Jens Mödeker

Fraunhofer FOKUS, Germany
{david.wagner,jens.moedeker}@fokus.fraunhofer.de

Abstract. The ability to dynamically adopt protocol functionality to the current situation will greatly improve performance, service availability and quality of service in the Future Internet. Nevertheless this provides a huge set of configuration and adaption options which have to be controlled intelligently and also in a timely manner. This creates need for a multi-level control and configuration framework. This paper presents a architecture for Dynamic Protocol Composition with some experimentation results and the design of a control and configuration framework that allows for efficient and reactive Protocol Composition and Execution while providing many options for configuration for a cognitive system and network management.

Keywords: Future Internet, dynamic protocol composition, cognitive network management, autonomic communication, communication protocols.

1 Motivation

The Internet as we know it is the result of thoughtful design that was supported by a repeated pattern of implementation and testing in the 1970's [1]. The fathers of the Internet decided to design the Internet Protocol as a narrow waist of oblivious datagram forwarding that avoids any connection state within the intermediate switching nodes. This decision paved the way to the Internet's success because it allowed the development of diverse novel applications and services on top of this very basic foundation. They also decided to protect state information from loss by gathering it at the endpoints of the net which are utilising the service of the network. Although this approach protects transport sessions against any number of intermediate failures, the limits and drawbacks of this design are apparent in today's networks: On one hand the simple mechanisms and assumptions of the Internet Protocol are being softened or even given up in many places, just think of middle boxes like firewalls, NAT-routers etc., VPNs, application proxies and so on. On the other hand devices, networks and service have become very heterogeneous, ranging from error-prone wireless sensor networks (WSNs) to multi-gigabit fibre-based storage area networks (SANs) but

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 334–345, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

today's protocols don't consider the special features or liabilities of the actual link. It becomes more and more apparent that today's Internet protocols, namely Transmission Control Protocol (TCP) [2] and User Datagram Protocol (UDP) [3], fail to offer a service that is acceptably close to the best possible service based on the optimal configuration of protocol functionality on each link on the path.

The rise of Autonomous Communication (AC) opens new opportunities because it allows the network management to make complex and fine-grained decisions in a cognitive manner. We identified two major subjects that would allow overcoming current limitations in a transparent and evolutionary way: First, protocol functionality should be managed in a dynamic way that allows taking into account changing context. Second, we propose to give up the end-to-end principle and to establish protocol functionality in intermediate nodes in the network. The management of functionality and soft state in the network seems to be feasible in the Future Internet using the intelligent features of Cognitive Network Management. Nevertheless completely new control and configuration architectures are needed that are able to cope with the very different requirements and situations.

2 Research on Dynamic Composition of Communication Protocols

The idea to compose protocol functionality according to requirements attracted Internet researchers very early in the 1990's and since has been researched for different motivations, with varying focuses and assumptions. In the beginning frameworks like the early x-kernel [4] have been developed which allowed building static protocols according to the actual needs. These protocols had to be developed, compiled and distributed in a static manner and did not allow for runtime changes. With time, the proposed architectures got more dynamic, proposals like DaCaPo [5], Protocol Boosters [6] or DiPS/CUPS [7] allow dynamic runtime reconfiguration of the protocol stack, CUPS even allows hot swapping of components [8]. The focus of the DaCaPo and DiPS/CUPS architectures is still on the end systems whereas the authors of the Protocol Boosters proposal already described the deployment of additional protocol functionality within the network. Nevertheless there were no results published and this idea was not further pursued. Although the authors expected protocol boosters to evolve fast because their transparency with respect to the end nodes they still assumed homogeneous deployment within an administrative domain.

3 Our Concept of Dynamic Protocol Composition

We think that Dynamic Protocol Composition Frameworks (DPCFs) can be designed to allow for compatible interoperation with legacy protocols, namely the IP-based protocols, while keeping the ability to deploy more elaborated functionality with other Dynamic Protocol Composition (DPC)-enabled nodes. In order to allow for highly efficient execution and minimal overhead the functional components, called Functional Protocol Elements (FPEs), handled by this framework shall be as small as reasonable: adding a sequence number, sending an acknowledgement or forwarding a packet are typical examples. This design goal leads to a fragmented world of micro-protocols which can be combined in a very efficient manner. Composed protocols can be tailored exactly to the needs of the service in a particular situation. To implement these composed protocols FPEs may express dependencies to other FPEs and even consist of a set of dependencies only, so called virtual FPEs (vFPEs). This allows single FPE instances and the respective header fields to be used to achieve several independent and more complex functionalities: A byte counter FPE can be used to achieve flow control at the same time as loss detection, maybe combined with automatic retransmissions.

It therefore is targeted on an efficient and highly dynamic packet handling which incorporates setting up of so called Functional Couplings like Automatic Repeat Request (ARQ) between nodes. To achieve this goal there is an architecture needed that on one hand allows fast and efficient packet processing but on the other hand allows for adaptation by the network management. These tasks can be supported by an efficient Self-Description mechanism that also supports abstract control interfaces by internally defining dependencies and conflicts and therefore allowing the DPC framework to solve many FPE related issues without external interaction.

The concept of minimal functional elements also facilitates the fine grained extension and adaptation of functionality within the network to the current situation in that local network: with such a framework it is possible e.g. to activate adding Forward Error Correction (FEC) to a (UDP-like) video streaming service for only the wireless last hop and at the same time activate local buffering and retransmissions for a reliable file transfer.

4 Applying DPC to Intermediate Nodes

The application of the principle of DPC to intermediate nodes i.e. routers creates new challenges in setting up and managing the DPC state in these nodes in an efficient and resilient manner. Current end-to-end protocols of the IP-based protocol family on purpose do not set-up any state in intermediate nodes which has several advantages, e.g. a clear separation of network management and end user equipment. Nevertheless a cognitive network management combined with soft state mechanisms (regularly refreshing signalling) will allow the use of DPC in the Future Internet. Applying communication functionalities, e.g. encryption or reliable transmission, dynamically between any nodes in the Future Internet allows to tailor the performance of each link to exactly the requirements of each flow and to the capabilities available in the current situation. We think that the potential benefit of more functionality within the network and the ability to adapt this functionality to the current context is promising a better network performance and higher efficiency. Therefore this topic is worth to be investigated more deeply.

5 Cognitive Control of Fine-Grained DPC Frameworks

Since DPC is only concept or tool to provide certain functionalities within a network, the management and the complexity of the management depend heavily on the goal that shall be achieved using this tool. Nevertheless some basic assumptions seem obvious and therefore lead our design of the management infrastructure. The first observation is that many decisions for (re-)configuration of DPC functionality require an understanding of the current network situation. To take the right decision, the decider has to know the exact location of a problem, e.g. on which link packets are lost, and, most important, has to determine the reason for the observed behaviour: packet loss may be induced by bad physical conditions but also by aggressive queuing strategies or overload of a link or a node. This also shows the need for continuous feedback in order to avoid amplification and oscillation in the network. Up to now there was no solution deployed fulfilling these requirements except the careful human administrator who intelligently gathers information, derives the current situation and the cause for the issue to be solved and then selects the action to be taken. Obviously this approach is not feasible for fine-grained protocol configurations and their frequent adaptations to changing network situations. The approach of cognitive network management or Autonomic Communication promises systems that are able to achieve a level of cognition that allows to assess the situation and to make intelligent decisions which take into account the expected impacts of the action to be taken. Therefore we assume situation awareness and cognitive decision making to be the key to successful broad and general deployment of DPC mechanisms.

Although the impact on our architecture is limited, we assume the hierarchical model of Cognitive System and Network Management (CSNM) presented in [9]. It is based on a Network Element Cognitive Manager (NECM) running on each Future Internet Element (FIE) that controls the node with respect to the capabilities that nodes provides. NECM makes self-aware and situation-aware decisions based on the local monitoring information available and the (expert) knowledge it stores. If decisions need information about greater parts of the network, e.g. topology and routing information, NECM may request a higher level cognitive manager, the Network Domain Cognitive Manager (NDCM), to take a decision. NDCM gathers high level information about its network domain and proactively takes decisions if it sees need for based on his information or reactively takes decisions if triggered by a NECM of its domain.

Although this concept promises intelligent decisions the effort needed to take a decision is high: Gathering information from many sources, deriving a situation, maybe predicting the impact of several execution options and the final decision enforcement is expensive with respect to time and computing resources. With respect to control of fine-grained DPC frameworks this is not acceptable for many minor communication decisions e.g. deciding on a session initiation request or on activation of Cyclic Reduncy Check (CRC) checking for a certain flow. Therefore we propose a more elaborated set of control interfaces which is presented in section 8. First, we present the underlying architecture that is controlled by this interfaces and show shortly potential advantages of DPC application on intermediate nodes.

6 The DPC Architecture and Implementation

The DPC implementation developed in the Self-NET project [10] provides a unified framework that replaces the Linux IPv6 protocol stack but runs as a user space application. This implementation is based on the C++ open source Simple and Extensible Network Framework (SENF [11]) and uses packet sockets to read and write packets. For signalling IPv6 extension headers are used which allow the DPC signalling to be transparent for legacy IPv6 nodes: the highest-order two bits of the used option type are set to zero, by this advising nodes that don't recognise this option to skip over it and continue processing.

The main objects of this framework besides packets are:

Functional Protocol Elements (FPEs). A FPE implements network protocol functionality. Some FPEs require the cooperation with other FPEs so these define dependencies in their Self-Description, vFPEs even consist of other FPEs only and don't implement own functionality at all. FPEs that don't have any dependencies are called basic FPEs and only these FPEs can be instantiated in Composed Protocol Chains (CPCs).

Packet Filters (PFs). A PF is defined by a set of packet attributes, so called Packet Filter Element (PFE) which partitions all packets into matches and not-matched. A simple example is a destination IPv6 network as it is used in routing rules. More complex examples use more attributes like source address, traffic class, flow label, transport protocol, port address etc. Two different filters are either disjoint, have a partial overlap or one includes the other. If two filters match a packet, the finer one will precede.

Composed Protocol Chains (CPCs). A CPC consists of a PF and an ordered chain of FPEs that defines what this nodes does with a packet that matches the PF. So a CPC defines a unidirectional protocol. It should be noted that this inherent support for unidirectional functionality definition allows DPC functionality to be tailored to the actual needs that often are asymmetric. Therefore two nodes will usually have different CPCs active if they are configured to provide a certain functionality in a collaborative way, e.g. when providing ARQ for a streaming service (shown in figure 3).

6.1 Components and Operation

An overview on the modules of the implemented DPC architecture and their interoperation is given in figure 1. The main components and their roles are introduced in the following:

The Packet Inspector (PI). This module checks an incoming packet for so called Active Information Elementss (AIEs) which trigger the reconfiguration / activation / deactivation of a specific FPE, e.g. a packet could contain a activate CRC-check flag.

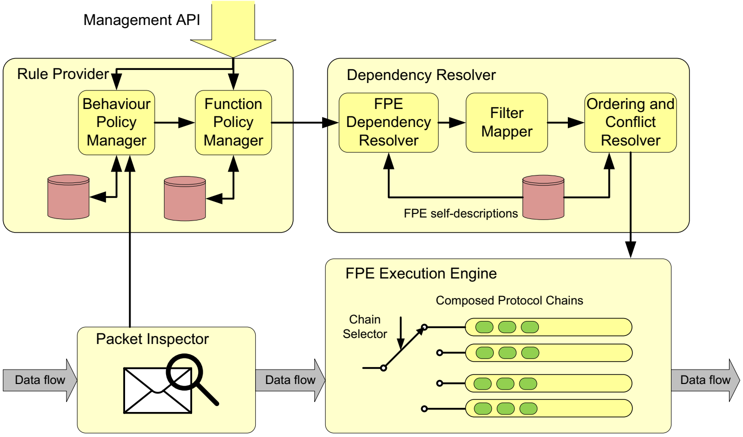


Fig. 1. Dynamic Protocol Composition Architecture

The Rule Provider (RP). This module manages two kinds of policies: **Function Policies** configure the application of a certain FPE for a certain PF and include routing rules, firewall rules, rules for adding or checking checksums, adding sequence numbers, triggering or sending acknowledgements etc. **Behaviour Policies** define how to decide on modification requests from other nodes received via AIEs (see section 8.2).

The Dependency Resolver (DR). This module composes the set of CPCs that is defined by the rule sets provided by RP. The process is detailed in section 9.

The FPE Execution Engine (FEE). This modules is responsible for the execution of the configured CPCs. For each incoming packet it selects the best matching filter, just like a router selects the longest matching prefix, and applies the FPEs in the order given by DR.

7 Initial Trials

In a first implementation step we implemented the basic components and six FPEs that allow two hosts to set up a ARQ functionality for the link or the path between them. The experimentation setup as depicted in figure 2 consists of seven Linux based PCs connected with Fast Ethernet. Two of them play the role of a streaming server and a streaming client and use a standard Linux IPv6 protocol stack. Four others, R1-R4, are equipped with the Fraunhofer DPC implementation and shall represent the routers of a wireless mesh network. The seventh computer V1 uses a standard Linux IPv6 protocol stack and allows to induce packet loss using the Linux kernel network emulation feature Netem [12].

In the experiment we start with a no loss and no DPC functionality except forwarding active on all routers. In a first step we induce 10% packet loss at

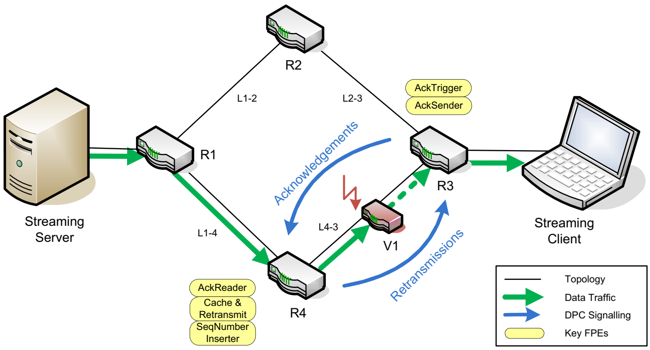


Fig. 2. Experimentation network setup

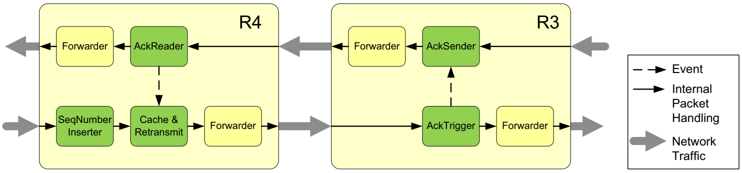


Fig. 3. CPC configuration when ARQ is enabled

V1. After some seconds we manually activate ARQ for transmissions from R4 to R3. This is implemented by two CPCs on R4 and two CPCs on R3, one sending and one receiving chain for this interface on each router. Please find the precise composition in figure 3.

7.1 Initial Results

Our first measurements are depicted in figure 4 and 5. In the monitored trial 10% packet loss (Gaussian distribution) have been induced at a time of 8.1 seconds on V1 resulting in a significantly increased packet loss as can be seen in figure 4. After 11.4 seconds the DPC framework activates a link ARQ mechanism which results in no packet loss but higher jitter. While before activation of DPC-based ARQ in figure 5 only one main cluster of delay can be recognised, after point 19.5 four clusters of delay can be recognised. These clusters represent packets that reach their destination after the initial transmission, the first automatic retransmission, the second or the third respectively.

The results show that certain properties of network performance can be significantly improved by the application of the DPC approach between routers. This solution provides several advantages compared to the usage of TCP since TCP causes acknowledgements and retransmissions to be forwarded along the complete end-to-end path.

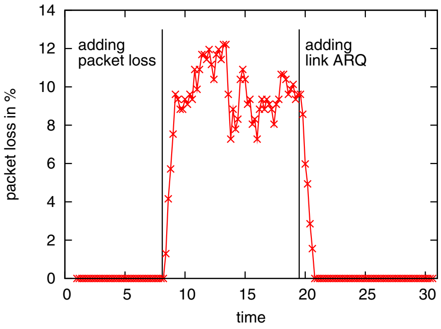


Fig. 4. Packet loss at receiver

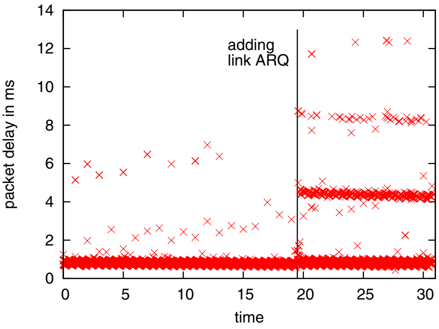


Fig. 5. Packet delay at receiver

8 Management of DPC Functionalities

As explained in section 5 it doesn't seem feasible to put all DPC-related decisions under direct control of the CSNM. The many different decisions required to control a dynamic communication protocol suite differ heavily in frequency, impact and immediacy. Our DPC architecture design exploits this fact and provides several options to take decisions that differ in the level of response time and intelligence with respect to situation awareness and cognition. All of decision making options base on the NECM who influences decisions taken within the DPC framework by providing preconfigurations that guide the decision. The four different ways of decision making considered in our DPC framework are presented in the following.

8.1 Reflex-Action Decisions

First, our architecture supports reflex-action decisions that are realised as preconfigured CPCs within the FEE component, e.g. to establish a connection when a request for a certain local service access point from a specified host or network is received. These CPCs are configured by the NECM inserting special Function Policies in the RP. The decisions on this level are prepared in advance and only wait for a trigger in form of a packet matching the PF of the CPC. Because of this lean structure they don't require significant computation time but the decision can only take into account information that can expressed in PFs, that means it is restricted to packet related information.

For security and resilience reasons we assume that a packet may only trigger configuration changes that apply for exactly the filter matching this packet: The configuration change will add or alter the CPC for exactly the PF of the triggering packet, i.e. the change will only affect packets coming from the same source address, same flow label etc. This postulation allows for flow-specific reconfigurations, in particular management of sessions while minimizing the risk of denial of service attacks. This new established state has to be refreshed periodically and is not part of the permanent ("hard") state which is stored in the RP.

Although these CPC-based decisions are very simple these rules are defined and can be changed at any time by the NECM who may use a very sophisticated situation aware cognitive and knowledge-based decision making framework which may even evaluate historical data and predictions.

8.2 Automated Rule-Based Decisions

The second option supported in our architecture is based on Behaviour Policies stored in the RP. These policies define rules for automated reconfigurations requested from other DPC-enabled nodes by a AIE and allow for a broader set of conditions as well as actions compared to the CPC-based rules described above. The Behaviour Policies may base on external configuration information the DPC framework can access fast, e.g. the current link speed of a WiFi interface. The result of a decision based on Behaviour Policies are Function Policies that define hard state of the DPC framework and are put into action as described in section 9.

Although the automated decision making mechanisms of this stage do not create situation awareness themselves, again it is the NECM who provides the Behaviour Policies to the Behaviour Policy Manager. The ability to define Behaviour Policies for the DPC framework allows NECM to define reactions for several expected situations that can be executed very fast based on a triggering message from neighbouring nodes and a certain set of context information. This system is expected to be used by the NECM to prepare for Functional Couplings like ARQ as described in section 7 with other DPC-enabled nodes.

Since the NECMs on R3 and R4 know that L4-3 is a wireless link which might be improved by Local ARQ, they prepare to serve as an ARQ-Acknowledger if requested. To take this decision NECM needs to know that the resources are sufficient to provide the additional service, e.g. bandwidth for the acknowledgements, computing power to check CRC and create acknowledgements etc.

8.3 Configuration by NECM

Third, our architecture provides a local management interface that allows configuration of the DPC framework by the local NECM. This interface to the RP is designed to store and retrieve the Function Policies that define the CPCs configuration. These policies define the “hard-state” of the DPC framework that e.g. would have to be restored in case of a reboot.

Since NECM provides the full set of cognitive features the policies configured using this interface are expected to represent high quality decisions without having strict immediacy. The interface was designed to allow for simple policies in contrast to the complex CPCs that are instantiated by the FEE. One FPE-policy consists of one PF and just one FPE which may be a virtual one. This keeps the configuration interface lean and is in line with the limited abilities of automated rule-based reconfigurations that are also stored in the Function Policy Manager.

8.4 Configuration by NDCM

The fourth control option is indirect management by the NDCM. The NDCM as a higher level cognitive manager has access to more information like topology, routing configuration, load and actual capabilities of the nodes in the network. This guarantees highest quality decisions but also leads to high delays and comparatively high costs for decision making and decision enforcement. Since NECM and NDCM communicate frequently we assume NECM to forward decisions taken by NDCM to the DPC framework using the interface described in section 8.3.

8.5 Comparison of Decision Making Levels

The proposed four levels of decisions vary in many properties. Table 1 gives a short overview on the most important properties of the four options.

Table 1. Properties of the different decision making levels

	CPC-based	**Rule-based**	**NECM-based**	**NDCM-based**
speed	++	+	–	– –
considered context	packet and CPC	simple local	local	compartment
level of cognition	– –	–	+	++
location of decision making	FEE	RP	NECM	NDCM
state affected	soft only	soft and hard	soft and hard	soft and hard
external signalling	inband	inband	outband	outband

The given rating of the speed of decision making on the different levels will be measured once the experimentation phase is concluded. When estimating the times between the trigger and the decision enforcement, the expected times lay between few microseconds for the CPC-based configuration changes up to many seconds or even few minutes for the decision to be taken by the NDCM. The given rating of level of cognition shall abstractly show the impact that the limited access to context and knowledge will have for the preconfigured automated decision processes in FEE and RP. This may be neglected except for abrupt changes in the network because the underlying rules, be it a policy in RP or a CPC in FEE, are defined with maximal knowledge and cognition.

Altogether the first two levels of decision making could not provide a sufficiently intelligent protocol configuration mechanism because the lack of knowledge and context information while NECM and NDCM alone could not achieve that goal because the required resources, in particular time. The combination of all four levels of decision making promises being able to deliver fast and intelligent decisions at the same time.

9 Handling of Policy Changes in the RP

Policy changes in RP may have different sources therefore measures have to be taken to guarantee the consistency of the protocol configuration in FEE and its consistency with the policies stored in the RP. Once changes are completed by a commit command, the resulting ruleset has to be checked for conflicts due to explicit incompatibility, ordering conflicts or contradicting parameters. The proposed architecture therefore realises the ACID properties [13] known from database transaction theory. The detailed process consists of three steps that are performed by subcomponents of the DR as depicted in figure 1.

FPE Dependency Resolution. In the first step for each policy the dependencies of the included FPE are resolved so that each rule is translated to a so called CPC description consisting of one PF, a set of FPEs and their parameters. The PFs of this set of CPC descriptions in general contains overlaps, inclusions and identity.

Filter Mapping. In the second step the Filter Mapper function resolves this diverse set of PFs to a tree consisting of internal nodes containing one PFE each and leafs containing a set of FPEs and their parameters. If two sets of FPEs have to be joined into one leaf because of overlapping PFs in the policies their parameters are checked for consistency. If they carry contradicting parameters, all changes are discarded and the process is rolled back. If the policy change request has been requested by the NECM, it is informed about the failure.

Ordering and Conflict Resolution. The third function is called when the tree is complete and works on the leafs only: The FPEs of each leaf are checked for conflicts and ordered according to their requirements expressed in their Self Description. In case of conflict or unresolvable position requirements, the processing of the set of policy changes is stopped and rolled back as described above.

If the policies could be merged, they are activated in FEE, stored in the RP and NECM is notified about the change.

10 Conclusion

The concept of applying DPC principles to intermediate nodes proves to be advantageous and the first experiments show that DPC allows to compensate packet loss and to greatly improve quality of service. The approach to focus on selected use cases and to research their aspects in detail has been productive and since the set of potential use cases and parameters is overwhelming, this approach should be continued for further research. In general the combination of DPC mechanisms with its many degrees of freedom with cognitive network management that allows to autonomously make situation-aware decisions based on knowledge is very promising and opens up many new opportunities to increase the efficiency of operating communication networks and by this save scarce resources like spectrum and energy.

Acknowledgement

The presented work is supported by the European Commission Seventh Framework Programme ICT-2008-224344 through the Self-NET Project [10].

References

1. Clark, D.: The design philosophy of the darpa internet protocols. In: SIGCOMM 1988: Symposium proceedings on Communications architectures and Protocols, pp. 106–114. ACM, New York (1988)
2. Postel, J.: Transmission Control Protocol. RFC 793 (Standard), Updated by RFC 3168 (September 1981)
3. Postel, J.: User Datagram Protocol. RFC 768 (Standard) (August 1980)
4. Hutchinson, N.C., Peterson, L.L.: The x-kernel: An architecture for implementing network protocols. IEEE Trans. Softw. Eng. 17(1), 64–76 (1991)
5. Vogt, M., Plattner, B., Plagemann, T., Walter, T.: A run-time environment for da capo. In: Leiner, B. (ed.) Proceedings of International Networking Conference, INET 1993, San Francisco, California, pp. BFC-1–BFC-9 (August 1993)
6. Feldmeier, D., McAuley, A., Smith, J., Bakin, D., Marcus, W., Raleigh, T.: Protocol boosters 16, 437–444 (April 1998)
7. Vcrbaeten, P., Janssens, N., Michiels, S.: Dips/cups: a framework for runtime customizable protocol stacks. Tech. rep. (2001)
8. Towards Hot-Swappable System Software: The DiPS/CuPS Component Framework (2002)
9. Mihailovic, A., Chochliouros, I.P., Kousaridas, A., Nguengang, G., Polychronopoulos, C., Borgel, J., Isral, M., Conan, V., Belesioti, M., Sfakianakis, E., Agapiou, G., Aghvami, H., Alonistioti, N.: Architectural principles for synergy of self-management and future internet evolution. In: Cunningham, P.C.M. (ed.) Proceedings of the ICT Mobile Summit 2009 (June 2009)
10. Self-NET (Self-Management of Cognitive Future InterNET Elements). EU FP7 project INFSO-ICT-224344, `https://www.ict-selfnet.eu`
11. The simple and extensible network framework, `http://senf.berlios.de`
12. Netem homepage, `http://www.linuxfoundation.org/collaborate/workgroups/networking/netem`
13. Haerder, T., Reuter, A.: Principles of transaction-oriented database recovery. ACM Comput. Surv. 15(4), 287–317 (1983)

Dynamic Call Admission Control for Enhanced GoS of UGS Connections during "Busy Hour" in WiMAX

Angelos Antonopoulos and Christos Verikoukis

Telecommunications Technological Centre of Catalonia
Parc Mediterrani de la Tecnologia (PMT) - Building B4
Av. Carl Friedrich Gauss 7, 08860
Castelldefels (Barcelona), Spain
{aantonopoulos,cveri}@cttc.es

Abstract. In this paper we introduce a dynamic connection admission control (CAC) mechanism for IEEE 802.16 broadband wireless access Standard. Our algorithm has been developed considering the problem of "busy hour" in communications traffic variation during a typical day. The proposed solution, which is compatible to the IEEE 802.16 Standard, provides higher priority to VoIP calls compared to other types of traffic in the network. The performance of the proposed algorithm is evaluated by means of computer simulations and compared to simple traditional admission control schemes.

Keywords: Admission Control, Busy Hour, WiMAX, IEEE 802.16, Medium Access Control (MAC).

1 Introduction

IEEE 802.16 Standard [1] was introduced in order to provide a Broadband Wireless Access (BWA), thus making it an attractive alternative solution to well-known wired technologies like xDSL and cable modem access. In the IEEE 802.16 architecture there are two types of stations: base station (BS) and subscriber station (SS). Each SS can serve a number of users who have access to the network. Both BS and SS are fixed, but inside the SS, users can be either static or mobile. Communication can take place in two different modes: Point-to-Multipoint (PMP) mode and Mesh mode. In PMP mode, the BS is the central entity that decides the transmission and reception schedules of the SSs, while in Mesh mode traffic can be routed directly between SSs without the need of BS. Our study is based on PMP architecture, where the communication path between BS and SS has two directions: uplink (from SS to BS) and downlink (from BS to SS), multiplexed either in time or frequency domain (TDD and FDD respectively).

Admission control is the mechanism that decides whether one new connection should be accepted or rejected, depending on network available resources. More

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 346–355, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

sophisticated admission control algorithms respect the QoS requirements of the connections in terms of delay, jitter and other network characteristics in order to provide a more reliable service to the end users [4],[5],[6].

In this paper, we propose a new connection admission control algorithm that gives priority to VoIP calls, especially during the "busy hour", when the arrival rate of the connections is the highest rate observed during the day. IEEE defines the "busy hour" as "the uninterrupted period of 60 minutes during the day when the traffic offered is the maximum" [11]. To the best of our knowledge, there is no proposed solution that tries to face the phenomenon of "busy hour", while the most of the work gives priority to real time services since they have been admitted by the system.

The rest of this paper is organized as follows. Section 2 provides an overview of IEEE 802.16 Medium Access Control (MAC) layer. Section 3 outlines the related work on admission control schemes for WiMAX networks in the literature. In Section 4 we introduce our proposed connection admission control method. The numerical results are provided in Section 5 and we conclude in Section 6 .

2 Overview of IEEE 802.16 Broadband Wireless Access (WiMAX) MAC Layer

2.1 Introduction

In this section we briefly review the mechanisms that IEEE 802.16 uses in order to provide the end user with quality of service.

Even though the physical layer specifications and the signaling mechanism for information exchange between BS and SS are well defined in the standard, the admission control and the resource allocation strategies have been left undefined, as it is shown in Figure 1.

2.2 Medium Access Control (MAC) Layer

IEEE 802.16 Medium Access Control layer, defined as connection-oriented, is designed to support different QoS requirements for different services. Based on that, the standard describes the following four types of services:

- Unsolicited Grant Service (UGS) is designed to support real-time service flows that generate fixed-size data packets (CBR traffic) on a periodic basis, such Voice over IP.
- Real-Time Polling Service (rtPS) is designed to support real-time service flows that generate variable sized data packets (VBR traffic) on a periodic basis, such as Moving Pictures Expert Group (MPEG) video.
- Non-Real-Time Polling Service (nrtPS) is designed to support non-real-time service flows that require variable size data grants, like File Transfer Protocol (FTP).
- Best Effort service (BE) is designed to provide efficient service for best effort traffic like Hyper-Text Transfer Protocol (HTTP)

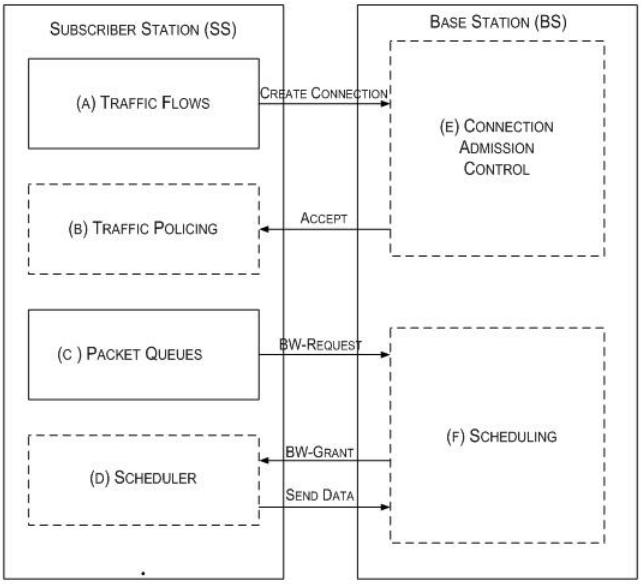


Fig. 1. IEEE 802.16 QoS Architecture

The traffic scheduler located at the BS decides on the allocation of physical slots in each time frame by considering the following parameters for each of the active connections:

- the scheduling service type that the connection belongs to;
- the QoS parameter values of the connection;
- the queue size of the data for transmission;
- the capacity of the available bandwidth.

2.3 Bandwidth Allocation and Request Mechanisms

Requests refer to the mechanisms that SSs use in order to notify the BS that they need bandwidth allocation for their upstream transmissions. There are two methods for transmitting bandwidth requests to the BS:

- Grant per Connection (GPC): Bandwidth is granted explicitly to each connection.
- Grant per Subscriber Station (GPSS): All connections from the same SS are treated as a single unit and bandwidth is allocated accordingly by the BS.

The latter case (GPSS) allows SS to distribute bandwidth among its connections, considering their QoS agreements, thus making it suitable for many connections per terminal, while the former case (GPC) is mostly appropriate for few users per SS.

3 Related Work

There have been some proposals presented in the literature to support QoS in IEEE 802.16 networks. Most of them focus on scheduling algorithms while only few face the connection admission control problem.

Wang et al. [2], proposed a dynamic admission control, using a degradation model as the number of connections increases. In [3], the authors suggest a hierarchical structure for bandwidth allocation, but they use a simple admission control that does not provide any guarantees in terms of delay and jitter.

To overcome this problem, the authors in [4] have proposed an admission control that uses priority queues, serving the UGS connections at first and providing delay and bandwidth guarantees to all the connections that have been admitted as well.

A predictive admission control algorithm is proposed by Castrucci et al. in [5]. The analysis that the algorithm performs anytime a new flow arrives, consists in (i) prediction of the network delay, (ii) comparison of the predicted delay with the delay threshold of the new flow and (iii) comparison with the delay threshold of the already accepted flows.

In [6], a new connection is admitted if there is enough bandwidth to accommodate it and the QoS of existing connections is maintained. The new connection receives QoS guarantees in terms of both bandwidth and delay.

An innovative work is presented in [7], concerning speech quality aware admission control. The proposed CAC, based on E-Model, has been designed considering the objective mouth-to-ear transmission quality.

In [8], the authors introduce an admission control and bandwidth allocation algorithm, based on game theory, considering Nash equilibrium for two players: BS and the new connection.

Finally, there have been some works in literature that try to evaluate the performance of admission control models in WiMAX networks [9], [10].

4 Dynamic Admission Control

As it derives from IEEE 802.16 service types, UGS flows are the most common way for daily communication, while the non-UGS flows are used to support web applications. Furthermore, recent studies have shown that the proportion of VoIP users will continue to grow from 28% of users in 2008 (up from 20% of users in 2007) to more than 50% in 2010 [13]. Due to that fact, our proposed CAC focuses in UGS flows, giving them higher priority comparing to the other three types of flows of the standard.

The problem becomes more intense if we take under consideration the variation of daily traffic volume, where there is a peak during the “busy hour” [11]. In Figure 2 the mean number of calls per minute to a switching centre taken as an average for periods of 15 minutes during 10 working days (Monday - Friday) is depicted. At the time of the measurements there were no reduced rates outside working hours [12].

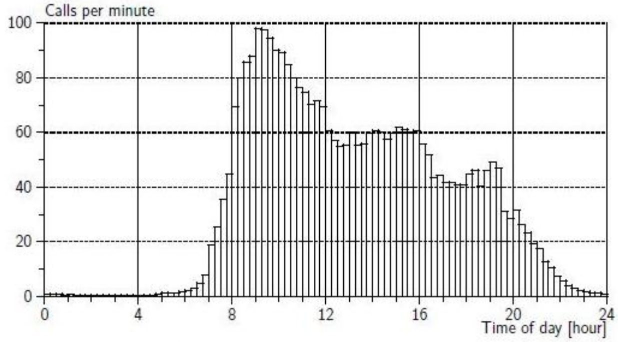


Fig. 2. Typical 24-hour traffic variation

It makes sense that we should give higher priority to VoIP calls during these hours, even if we have to reject some requests from the rest flows, under certain conditions.

The target of the proposed connection admission control algorithm is to provide enhanced Grade of Service (GoS) to VoIP calls, by improving the acceptance rate of the UGS flows. Grade of Service is defined as the probability of a call being blocked or delayed more than a specified interval. From a practical aspect it could also be defined as the probability of a user receiving a network busy signal in a telephone service and can be measured using the following equation:

$$GoS = \frac{Number\_of\_lost\_calls}{Number\_of\_offered\_calls} \tag{1}$$

Using our CAC, the BS accepts all the UGS flows if the available bandwidth suffices, in order for the flows to be served. In case of rtPS and nrtPS flows there is a blocking probability that depends both on the arrival rate of UGS requests and on the available bandwidth as well. In order to deal with BE connections, the requests are always admitted. However, no bandwidth allocation is considered, since BE flows do not need any QoS guarantees.

It is clear that during the “busy hour” the arrival rate of UGS flows is the highest rate observed during the day, thus we may have to reject some requests coming from the other service types, although there is enough bandwidth for them to be served. Moreover, it is common that the daily traffic variation establishes our ability to predict an increase in VoIP calls. Still, taking into consideration the above, we are obliged to reserve the system resources.

The proposed connection admission control algorithm has two parameters: the arrival rate of UGS requests and the available bandwidth of the system. The blocking probability for the other connections increases either when the arrival rate of the VoIP requests increases or when the available bandwidth decreases. We approximately estimate the capacity we need in order to serve all the upstream connections using the following type:

$$C_{need} = \sum_{i=UGS,rtPS,nrtPS} \rho_i \times B_i \tag{2}$$

In the above expression, ρ_i, defined as traffic intensity, is a measure of the average occupancy of the base station during a specified period of time. It is denoted as $\rho_i{=}\lambda_i/\mu_i$, where λ_i is the arrival rate for each flow and μ_i represents the mean service rate, while B_i is the bandwidth needed for each type of connection. The index i corresponds to different service types and can take values {UGS, rtPS, nrtPS}.

In case that the system bandwidth suffices to serve the flows of all service types, the blocking probability equals zero. Due to this fact, the proposed admission control has the same output with classic admission control schemes under conditions of light traffic in the network. On the contrary, in overloaded environments where the bandwidth is not sufficient for all the connections, we should use an admission control algorithm in order to give different levels of priority to the various connections.

The arrival rate of the UGS requests can be defined as λ_{UGS}. If this rate is higher than one specific threshold there will be a blocking probability for the requests of the other service types. This threshold is defined by the administrator / operator of the network, by considering the network parameters, as the arrival rate of VoIP calls during "busy hour". The values' range of this probability fluctuates between $Pblock_{min}$ and $Pblock_{max}$, depending on the available bandwidth of the system. In the extreme case when we have no available bandwidth the overall blocking probability becomes $Pblock_{max}$. To the contrary, when the total bandwidth of the system is available and no connections are being served, i.e. $BW_{available}/BW_{total} = 1$, the blocking probability becomes $Pblock_{min}$, as there is enough bandwidth in order for the connections of all types to be served. These borderline values are selected by the system's operator according to each traffic class' desired level of priority. On the other hand, whenever the arrival rate of UGS connections is smaller than this arrival rate threshold, we assume that we are off "busy hour" and, therefore, the blocking probability equals zero. The pseudo-code of the proposed Call Admission Control algorithm is presented in TABLE 1.

5 Performance Results

In order to evaluate the performance of our CAC algorithm we have developed an event driven C++ simulator. Simulations have been carried out, assuming a WiMAX - OFDMA physical interface between BS and SSs, using the TDD duplexing technique, a channel bandwidth of 10MHz and 1024 subcarriers. The frame duration is 5 msec and the OFDMA symbol duration of 102.86 μsec. The modulation scheme chosen for downlink and uplink direction is 16-QAM with code rate 3/4. In this section we present the simulation set up and results of our experiments.

Table 1. Dynamic Admission Control Algorithm

```
Algorithm. Dynamic Admission Control
$C_{need} = \rho_{UGS} \times B_{UGS} + \rho_{rtPS} \times B_{rtPS} + \rho_{nrtPS} \times B_{nrtPS}$
    if (arrival_rate ≥ threshold) then {
        if(total_BW ≥ $C_{need}$ )
            $P_{blocking} = 0$
        else if (total_BW < $C_{need}$ ){
            Rate_of_available_BW = available_BW / total_BW
            Fixed_rate = Rate_of_available_BW/4 %% normalize the value between 0-0.25 %%
            Dependence = 0.25 - Fixed_rate
            $P_{blocking} = Pblock_{min}$ + Dependence }}
    else if(arrival_rate < threshold) %% when we are off “busy hour”,$P_{blocking}$ becomes zero %%
            $P_{blocking} = 0$
```

5.1 Simulation Scenario

We assume that the arrival rate of requests for new connections follows a Poisson distribution with mean value 1 connection/sec (because of the traffic intensity), while the service time is exponentially distributed with mean time 60 and 50 seconds for the UGS and the rest flows respectively. For simplicity, but without the loss of generality, we treat the two flows (rtPS, nrtPS) as one with the same characteristics (i.e. arrival rate, bandwidth demand). In this point we must clarify that this simplification concerns only the admission control process since, after being accepted, the two classes are treated according to their different priorities. Furthermore, as we have already mentioned, BE connections are always admitted in the system, without any QoS guarantees.

Using the physical layer that was described above, we derive an overall bandwidth of 4 Mb/s for the uplink traffic, while the bandwidth that each rtPS / nrtPS connection uses is 128 kb/s. The codec chosen to generate VoIP traffic is the G.711, resulting to a constant bit rate of 64 kb/s. The system parameters are presented in Table 2.

Under these assumptions, the system can serve about 98% of the UGS calls, if all the requests of the other classes are rejected, which means that we have an over-loaded simulation environment. In the specific case where all the requests

Table 2. System Parameters

Bandwidth	4Mb/s
λ_{UGS}	Poisson(1 connection/sec)
$\lambda_{rtPS,nrtPS}$	Poisson(1 connection/sec)
$1/\mu_{UGS}$	Exponential (60 sec)
$1/\mu_{rtPS,nrtPS}$	Exponential (50 sec)
B_{UGS}	64kb/s (G.711)
$B_{rtPS,nrtPS}$	128kb/s
Threshold	0.2 calls/sec
Pblockmin	0.6
Pblockmax	0.85

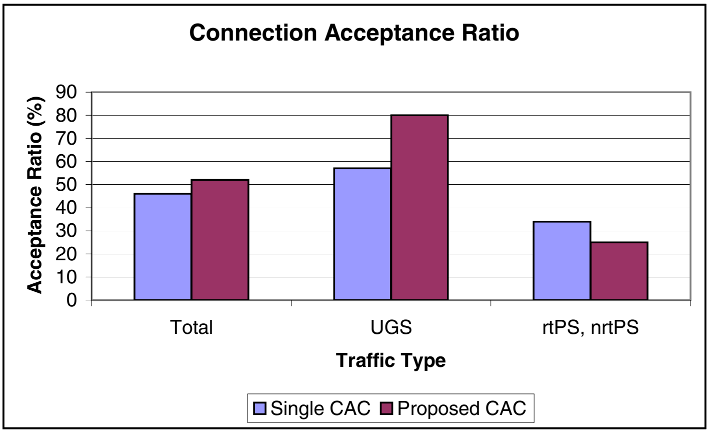


Fig. 3. Flow Acceptance Ratio for all classes of traffic

are being accepted if there is enough bandwidth, no matter the class that they belong to, the system serves about 57% of the UGS flows and 34% of the other flows.

Our aim is to serve more VoIP calls by reducing the Grade of Service of the UGS connections. Simulation results showed that, using our CAC, we can increase the served VoIP calls up to 80% which is a significant enhancement comparing to 57% we have without using this algorithm. At the same time, the ratio of the accepted connections of the rest two classes decreases to 25%, but this makes sense as our aim is to give priority to UGS flows (Figure 3).

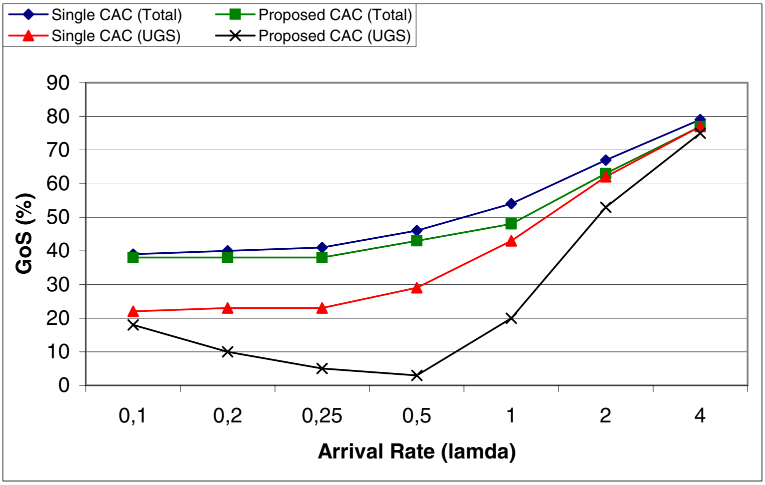


Fig. 4. Grade of Service vs. UGS Connections Arrival Rate

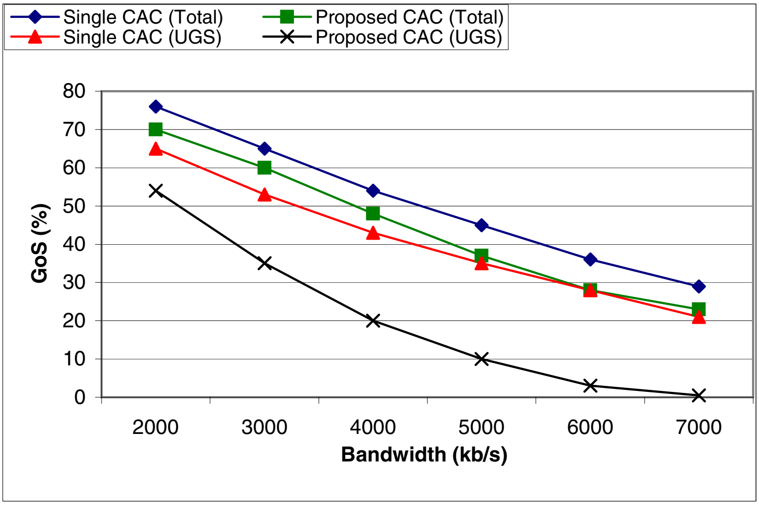


Fig. 5. Grade of Service vs. Total Bandwidth

Comparing our proposed dynamic admission control to traditional schemes for different values of arrival rates for the UGS connections, we observe that our CAC outperforms single admission control methods, without any deterioration in the overall system performance. Figure 4 depicts the Grade of Service among various arrival rates of UGS connections. It is observed that, using our proposed CAC, a better system performance in terms of VoIP communication is achieved, as there is a significant enhancement in GoS (2-26%) of UGS connections. Furthermore, the overall system performance is improved as the acceptance ratio of the total number of connections is increased. As far as networks with restricted bandwidth capabilities are concerned, we observe that the proposed dynamic admission control is superior to single methods for different values of system bandwidth. In Figure 5 the GoS for various values of system bandwidth is presented. In all cases the proposed CAC outperforms single admission control schemes, as it improves the GoS both for UGS connections (11-23%) and for the total number of connections (6-8%) as well.

6 Conclusion

In this paper, a new connection admission control algorithm for IEEE 802.16 architecture is presented. Compared to simple admission control methods, the proposed solution improves the Grade of Service of UGS connections, as the Base Station serves more VoIP calls by considering the “busy hour” phenomenon. In order to achieve better results in terms of QoS requirements, CAC should be accompanied by an optimum transmission scheduling. In our future work we shall focus our research on such issues.

References

1. IEEE Standard, IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed Broadband Wireless Access System, IEEE Std 802.16-2004 (June 2004)
2. Wang, H., Li, W., Agrawal, D.P.: Dynamic Admission Control and QoS for 802.16 Wireless MAN. In: IEEE Wireless Telecommunications Symposium, pp. 60-66 (April 2005)
3. Chen, J., Jiao, W., Wang, H.: A Service Flow Management Strategy for IEEE 802.16 Broadband Wireless Access Systems in TDD Mode. In: IEEE International Conference on Communication, ICC 2005 (2005)
4. Chandra, S., Sahoo, A.: An efficient call admission control for IEEE 802.16 networks. In: Proc. IEEE Workshop on Local and Metropolitan Area Networks (LANMAN), New Jersey, USA, pp. 188–193 (June 2007)
5. Castrucci, M., Delli Priscoli, F., Buccella, C., Puccio, V., Marchetti, I.: Connection Admission Control in WiMAX networks, White Paper
6. Wongthavarawat, K., Ganz, A.: Packet Scheduling for QoS Support in IEEE 802.16 Broadband Wireless Access Systems. International Journal of Communication Systems 16, 81–96 (2003)
7. Bohnert, T.M., Staehle, D., Kuo, G.-S., Koucheryavy, Y., Monteiro, E.: Speech Quality Aware Admission Control for Fixed IEEE 802.16 Wireless MAN. In: ICC 2008, IEEE International Conference on Communications, May 19-23, pp. 2690–2695 (2008)
8. Niyato, D., Hossain, E.: A game-theoretic approach to bandwidth allocation and admission control for polling services in IEEE 802.16 broadband wireless networks. In: Proceedings of the 3rd international conference on Quality of service in heterogeneous wired/wireless networks, Waterloo, Ontario, Canada, August 07-09 (2006)
9. Kwon, E., Lee, J., Jung, K., Ryu, S.: A Performance Model for Admission Control in IEEE 802.16. In: Braun, T., Carle, G., Koucheryavy, Y., Tsaoussidis, V. (eds.) WWIC 2005. LNCS, vol. 3510, pp. 159–168. Springer, Heidelberg (2005)
10. Ghazal, S., Mokdad, L., Ben-Othman, J.: Performance Analysis of UGS, rtPS, nrtPS Admission Control in WiMAX Networks. In: ICC 2008, IEEE International Conference on Communications, May 19-23, pp. 2696–2701 (2008)
11. Weber, J.: Dictionary of English Language Traffic Terms. IEEE Transactions on Communication Technology 16(3), 365–369 (1968)
12. Iversen, V.B.: Analysis of real teletraffic processes based on computerized measurements. Ericsson Technics (1), 1–64 (1973); Holbk measurements
13. Report Study, Enterprise VoIP Market Trends 2009-2012. Osterman Research Inc. (February 2009)

Mutual Information Effective SNR Mapping Algorithm for Fast Link Adaptation Model in 802.16e

Fernando López Aguilar, Gorka Rubio Cidre, José Manuel López López,
and Javier Regidor Paris

Telefónica I+D
Emilio Vargas, 6, 28043 Madrid, Spain
`{fla,gorka,joseml1,javirp}@tid.es`

Abstract. The Always Best Connected Systems (ABCS) philosophy, in which different access technologies coexist, allows the user to select at any time an appropriate network that is optimized for the current service. To study this scenario through simulations, it is needed that all simulators are system-level type. Regarding this point, Effective SNR Mapping (ESM) algorithms provide the link layer abstraction that is crucial for the system level simulation interface. In this paper we have used the Mutual Information Effective SNR Mapping (MI-ESM) algorithm for instantaneous-channel modelling, calibration and evaluation of the Link Level Interface in the WiMAX System 802.16e together with a realistic Mobile WiMAX simulator. Plenty of simulations were performed to evaluate different algorithms and the results show that MIESM gives higher accuracy than the rest of ESM methods.

Keywords: Link layer abstraction, effective *SNR*, MIESM, 802.16e, Mobile WiMAX, H-ARQ, AMC and PUSC/FUSC.

1 Introduction

In OFDM (Orthogonal Frequency Division Multiplexing) Multi-Carrier simulators, the system level usually interfaces with the link level using SNR (Signal to Noise Ratio) Mapping methods. As a result, complexity is reduced and performance benefits from shorter simulation times. Mapping methods surpass classical methods from the calibration point of view, characterizing each Modulation and Coding Scheme (MCS) in multipath channels taking into account shadowing, Doppler Effect, reception diversity and other effects that deteriorate the transmission.

Although most works in literature deal with OFDM aspects, our work aims at realistic simulations of 802.16e. Special aspects such as H-ARQ (Hybrid Automatic Repeat Request), Partial Use of Sub-Carriers (PUSC)/Full Use of Sub-Carriers (FUSC) permutations and AMC (Adaptive Modulation and Coding) play an important part in our simulations. As for the calibration phase, the MIESM (Mutual Information Effective SNR Mapping algorithm) is used. The ultimate goal is to reach calibration results that accurately match real situations.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 356–367, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

The link-to-system mapping look-up table is built following the procedure shown in Fig. 1 [3]. For each MCS, simulations are performed over a wide range of effective SNR to estimate the block error rate, the calibration factor (β) and the mean square error.

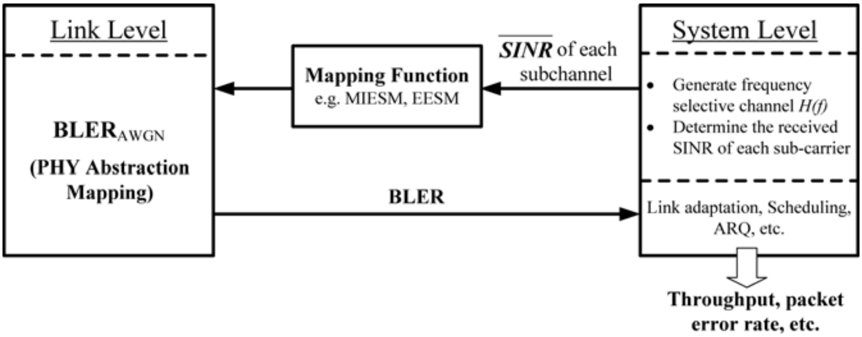

Link Level
BLER$_{AWGN}$
(PHY Abstraction Mapping)
Mapping Function
e.g. MIESM, EESM
$\overline{SINR}$ of each subchannel
BLER
System Level
Generate frequency selective channel $H(f)$
Determine the received SINR of each sub-carrier
Link adaptation, Scheduling, ARQ, etc.
Throughput, packet error rate, etc.

Fig. 1. Link-to-system mapping procedure

The rest of the paper is organized as follows. Section 2 describes the link level simulator. Section 3 reviews the Mutual Information Effective SNR Mapping algorithm to be used in conjunction with the simulator. The simulation parameters and results are presented and analyzed in Section 4. Finally, section 5 summarizes the conclusions and foresees future work on the subject.

2 Description of the Mobile WiMAX Link Level Simulator

The Mobile WiMAX Simulator, whose architecture is shown in Fig. 2, is a standalone application compiled in Visual C++ for Windows, that seeks to emulate a single link (the first two layers, physical and MAC –Media Access Control–) of this broadband wireless solution (IEEE 802.16e), that will play a key role in metropolitan area networks, enabling the convergence of mobile and fixed broadband radio access technologies and flexible network architecture. Mobile WiMAX systems offer scalability in both radio access technology and network architecture, thus providing a great deal of flexibility in network deployment options and service offerings.

The IEEE 802.16e Wireless MAN OFDMA mode [9] is based on the concept of scalable OFDMA (S-OFDMA). S-OFDMA supports a wide range of bandwidths to flexibly address the need for various spectrum allocation and usage model requirements. The scalability is supported by adjusting the FFT (Fast Fourier Transform) size while fixing the sub-carrier frequency spacing at 10.94 kHz.

This technology supports sub-channelization in both Down Link (DL) and Uplink (UL), and there are two types of sub-carrier permutations for sub-channelization: diversity-based and contiguous. The diversity permutation draws sub-carriers pseudo-randomly to form a sub-channel. It provides frequency diversity and inter-cell interference averaging. The diversity permutations include DL FUSC (Fully Used Sub-Carrier), DL PUSC (Partially Used Sub-Carrier), UL PUSC and additional optional permutations such as Adaptive Modulation and Coding (AMC). With DL PUSC, for each pair of OFDM symbols, the available or usable *sub-carriers* are grouped into *clusters* containing 14 contiguous sub-carriers per symbol period, with *pilot* and *data* allocations in each cluster in the even and odd symbols. The available sub carrier space is split into *tiles* and six *tiles*, chosen from across the entire spectrum by means of a re-arranging/ permutation scheme, and grouped together to form a *slot*. The *slot* comprises 48 data sub-carriers and 24 pilot *sub-carriers* in 3 OFDM symbols. The contiguous permutation groups a block of contiguous *sub-carriers* to form a *subchannel*. The contiguous permutations include DL AMC and UL AMC, and have the same structure. A *bin* consists of 9 contiguous *sub-carriers* in a *symbol*, with 8 assigned for *data* and one assigned for a *pilot*. A *slot* in AMC is defined as a collection of *bins* of the type (N x M = 6), where N is the number of contiguous *bins* and M is the number of contiguous *symbols*. Thus the allowed combinations are [(6 *bins*, 1 *symbol*), (3 *bins*, 2 *symbols*), (2 *bins*, 3 *symbols*), (1 *bin*, 6 *symbols*)]. AMC permutation enables multi-user diversity by choosing the subchannel with the best frequency response.

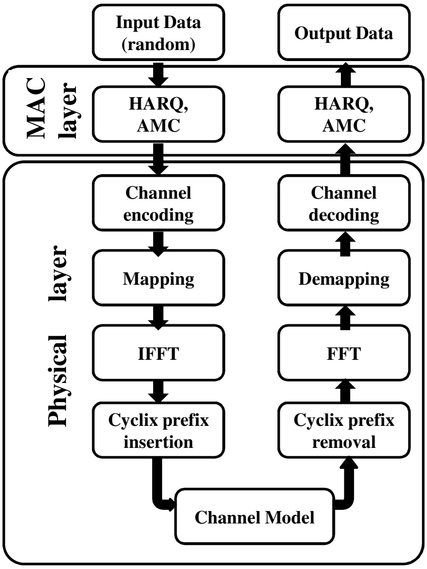


Fig. 2. Architecture of Mobile WiMAX Simulator

In general, diversity *sub-carrier* permutations perform well in mobile applications while contiguous *sub-carrier* permutations are well suited for fixed, portable, or low mobility environments. These options enable the system designer to trade-off mobility for throughput.

H-ARQ is supported by Mobile WiMAX. H-ARQ is enabled using an N channel "Stop and Wait" protocol which provides fast response to packet errors and improves cell-edge coverage. Chase Combining and optionally Incremental Redundancy are supported to further improve the reliability of the retransmission. A dedicated ACK channel is also provided in the uplink for H-ARQ ACK/NACK signalling. Multi-channel

H-ARQ operation is also supported. Multi-channel stop-and-wait ARQ with a small number of channels is an efficient, simple protocol that minimizes the memory required for H-ARQ and stalling. WiMAX provides signalling to allow fully asynchronous operation. The asynchronous operation allows variable delay between retransmissions which gives more flexibility to the scheduler at the cost of additional overhead for each retransmission allocation. H-ARQ, combined together with CQICH (Channel Quality Indicator CHannel) and AMC, provides robust link adaptation in mobile environments at vehicular speeds in excess of 120 km/h.

Rayleigh fading is the statistical model used in this simulator, which emulates the effect of shadowing, multipath, Doppler and cross polarization discrimination (XPD), also taking into account advanced techniques such as diversity reception and antenna correlation. All these parameters, together with mobile terminal speed, are fixed initially in the simulator before starting the simulation.

Finally, we use a frequency selective wireless channel that can be modelled by a tapped delay line channel model (time-variant Finite Impulse Response –FIR– filter in complex equivalent low-pass signal domain). The number of FIR taps is given by the power delay profile of the channel, or the r.m.s. (root mean square) delay spread of the channel. Both are configured at the beginning of the simulation. Each of the complexes FIR taps changes over time. The time delays between the multipath components depends on both the surrounding reflectors and the antennas involved, imposing a distinction among propagation paths between base stations and propagation paths from a base station to the users. Depending on the antennas used and the transmission environment, multipath components with significant delay spreads will occur. The amplitude (in dB) of each FIR tap has the statistics of a Rayleigh random process, and the way it changes over time is determined by the Doppler spectrum of the channel, where the relative motion between base station and mobile terminal (or surrounding objects causing e.g. reflection) causes random frequency modulation, since each multipath component has a different Doppler shift (phase change per time unit). Known the influence on the system performance of specific antenna characteristics (radiation pattern, polarization characteristics, cross-polarization discrimination) in MIMO (Multiple Input Multiple Output) systems, the radio link takes into account the XPD of the antennas.

3 Review of Mutual Information Effective SNR Mapping Algorithm

The link-to-system mapping methods can be effectively used in OFDM communication systems through using the effective SNR concept [2][10]. Some of these methods are based on Mutual Information metrics. The MIESM algorithm defines the mutual information on the bit channel itself, which we will refer to as the mutual information per coded bit to build the optimized function for each modulation scheme.

A block diagram for the MIESM approaches is shown in Fig. 3. Given a set of N received encoder symbol SINRs (Signal to Interference-plus-Noise Ratios) from the system level simulation, denoted as $SINR_1, SINR_2, SINR_3, \ldots, SINR_N$, a mutual information metric is computed. Based on the computed MI-metric an equivalent SINR is obtained and used to look-up the BLER (BLock Error Rate).

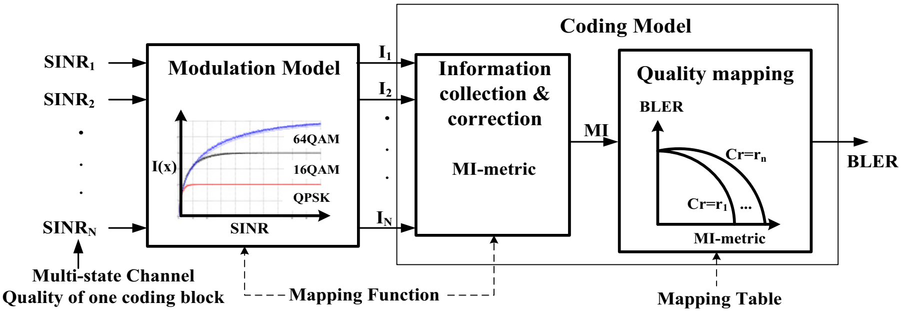


Fig. 3. Effective mapping abstraction procedure

The computation of MIESM is based on the nonlinear mapping relationship from *SINR* to mutual information to calculate the effective *SINR*, as we can see in equation (1)[2], in which β is a calibration factor whose value is chosen to minimize the root mean square (r.m.s) error between the effective SNR, derived from the Rayleigh channel, and the static SNR which leads to the same BLER value:

$$SNR_{eff} = \beta \cdot I^{-1}\left(\frac{1}{P}\sum_{p=1}^{P} I\left(\frac{SINR_p}{\beta}\right)\right) \tag{1}$$

Here, I is the mutual information function, taking into account the modulation type. The obtaining of I is based on equation (2), in which m_p is the bits per symbol, X is the set of symbols, ${X_b}^i$ is the set of symbols for which bit i equals b. Y is a zero mean unit variance complex Gaussian random variable.

$$I_{m_p} = m_p - E_y\left\{\frac{1}{2^{m_p}}\sum_{i=1}^{m_p}\sum_{b=0}^{1}\sum_{z\in X_b^i} log_2 \frac{\sum_{\hat{x}\in X} e^{-\left|Y-\sqrt{x}(\hat{x}-z)^2\right|}}{\sum_{\tilde{x}\in X} e^{-\left|Y-\sqrt{x}(\tilde{x}-z)^2\right|}}\right\} \tag{2}$$

This equation provides the curves shown in Fig. 4. Hence the constellation points of 16-QAM and 64-QAM are normalized by a factor to ensure that the average energy over all symbols is one. Curves are compared against the IEEE reference model [3].

Detailed below are the needed steps to obtain the SNR_{eff} and the optimal β based on the equation (1) and (2):

Step 1. Obtain the BLER vs. SNR curve for an Additive White Gaussian Noise (AWGN) channel.

Step 2. Obtain a high number of BLER vs. SNR curves for a tapped delay Rayleigh channel (3GPP Extended Pedestrian A –EPA– channel model) performing simulations. Gather SNR per subcarrier data as part of the simulations.

Step 3. Find the BLER values obtained in Step 2 (Rayleigh) into the AWGN curve. We called this SNR_{static_S} where S is the number of simulated points (Number of curves for EPA channel model multiplied by the number of points of each curve).

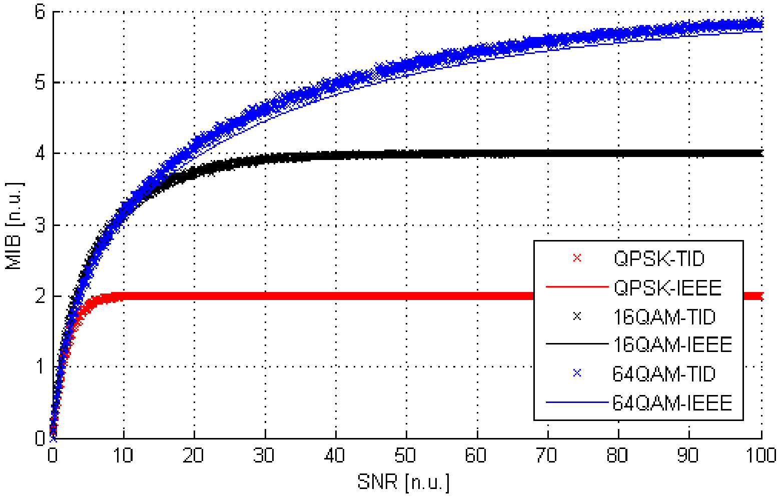


Fig. 4. MIB vs. SNR, both calculated by us and modelled by IEEE

Step 4. For each SNR_{static_S} value, we know the associated value of BLER, SNR evaluated and the SNR per subcarrier (SINR$_P$). The SNR per subcarrier will be translated into a SNR effective (SNR_{eff_S}, where S is the number of simulated points) with the appropriate equation for MIESM algorithm described below. This SNR_{eff} is a function which depends on β and I. The key formula used has been shown in (1).

Step 5. Finally, we iterate for a large range of β values to obtain the optimal β through the minimization of the root mean square error (r.m.s) between SNR_{eff_S} and SNR_{static_S}. This is calculated using equations (3) and (4):

$$r.m.s. = \frac{1}{S}\sum_{s=1}^{S}\left(SNR_{eff_s} - SNR_{static_s}\right)^2 \tag{3}$$

$$\beta = \arg min(r.m.s.) \tag{4}$$

4 Simulation Results

In this section, we verify the abstraction algorithm performance. The multipath channel mode considered is EPA, as is specified in [7], at pedestrian speed (3 km/h). The tapped delay line model used in our Rayleigh simulations is shown in Fig. 5.

The simulation was performed in the frequency domain using 360 data sub-carriers spaced 10.94 KHz. For each channel realization there are 2000 simulated frames. The PUSC permutation schemes [8] have the advantages of distributed subcarrier allocation and are well suited for mobile, fast-moving subscribers. Incremental-Redundancy- based H-ARQ is selected taking the puncture pattern into account, and for each retransmission the coded block is not the same. We also use H-ARQ due to the fact that it provides a significant advantage throughout the range of practically relevant SNRs. In addition, incremental redundancy is selected because it is shown to outperform lower-complexity Chase combining, particularly at moderate and high SNRs. The whole configuration parameters of the simulation can be seen in Table 1.

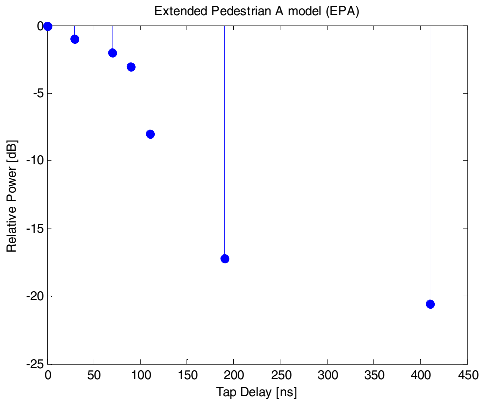


Fig. 5. 3GPP Extended Pedestrian A model EPA (Tapped Delay Channel) Multi-Path Environments with Classic Doppler Spectrum.

Table 1. Link Level Simulator Parameters

Parameter	Value
Carrier Frequency	3.5GHz
Bandwidth	5MHz
Sub-Carrier Spacing	10.94KHz
Sampling Frequency	5.6 MHz
FFT Size	512
Number of Sub-Channels	8
Useful Symbol Time	91.4 µs
Guard Time	11.4 µs
OFDMA Symbol Duration	102.9 µs
Null Sub-Carriers	92
Pilot Sub-Carriers	60
Data Sub-Carriers	360
Sub-Channels	15

Parameter	Value
Symbol Period, Ts	102.9µs
Frame Duration	5ms
OFDM Symbols/Frame	48
Data OFDM Symbols	44
Permutation	PUSC
Simulated Frames	2000
XPD	10 dB
Channel Estimation	Real (Pilots)
H-ARQ	Incremental Redundancy
Power Delay Profile	AWGN and EPA channel model, Extended Typical Urban (ETU) [7]
Mobile speed	Pedestrian (3Km/h)
Antenna Scheme	SIMO Correlated Antennas. Diversity Reception (10dB)

The different Modulation Coding Schemes (MCS) used are defined based on Modulation, Coding Rate using Turbo Code Codification and Repetition Factor[9]. The possible options are shown in Table 2.

Table 2. Transmission mode parameters

Modulation	Coding Rate	Repetition Factor	Modulation Coding Scheme
QPSK	½ CTC	x6	MCS1
	½ CTC	x4	MCS2
	½ CTC	x2	MCS3
	½ CTC	x1	MCS4
	¾ CTC	x1	MCS5
16QAM	½ CTC	x1	MCS6
	¾ CTC	x1	MCS7
64QAM	½ CTC	x1	MCS8
	2/3 CTC	x1	MCS9
	¾ CTC	x1	MCS10
	5/6 CTC	x1	MCS11

Fig. 6 shows the result of the execution of Step 1 (reference curves for all MCS) as we explained in Section 3. The different modes are shown in ascendant order based on Table 2 with a spatial separation of approximately 2dB. Red lines correspond to QPSK modulation, green lines correspond to 16QAM and blue lines correspond to 64QAM.

Although Fig. 7 is not necessary to calculate β, we show it in order to validate our whole simulation process. The Downlink Rate obtained is almost the same as the theoretical values [9].

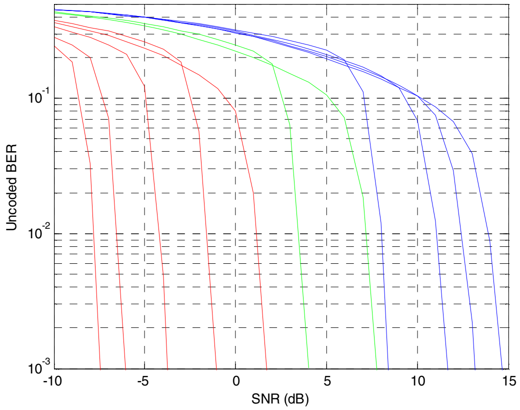


Fig. 6. Uncoded BER vs. SNR for different transmission modes in AWGN channel @ 3km/h

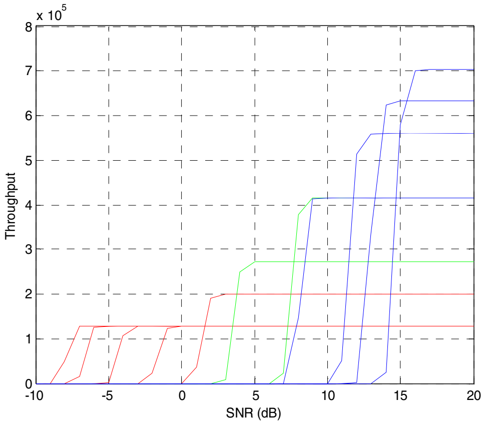


Fig. 7. Link level throughput with HARQ in AWGN channel @ 3km/h

Table 3 shows *β* and r.m.s error values obtained for the MIESM algorithm evaluated in this paper and the ESM methods described in [1]. These values are obtained using the formulas described in Section 3.

Table 3. β and r.m.s. error values for different MCSs in MIESM

MCS	β_{MIESM}	error	β_{EESM}	error	β_{CESM}	error	β_{LESM}	error
1	1.03	0.010	1.68	0.055	0.08	0.165	-0.29	0.090
2	1.07	0.015	1.71	0.017	0.09	0.121	-0.24	0.015
3	1.11	0.019	1.73	0.023	0.12	0.228	-0.22	0.020
4	1.15	0.021	1.75	0.121	0.16	0.218	-0.19	0.117
5	1.18	0.028	1.78	0.055	0.19	0.153	-0.17	0.056
6	1.09	0.026	5.29	0.088	0.23	0.183	-0.16	0.090
7	1.13	0.018	7.51	0.102	0.03	0.188	0.27	0.175
8	1.06	0.017	12.57	0.087	0.05	0.291	0.29	0.079
9	1.12	0.011	16.21	0.120	0.09	0.225	0.35	0.122
10	1.16	0.013	27.27	0.139	0.12	0.370	0.39	0.169
11	1.17	0.014	32.14	0.178	0.15	1.180	0.44	0.196

It is noticeable that r.m.s error and *β* values do not increase if MCS modes go higher. Comparing MIESM to other ESM algorithms (EESM, CESM and LESM) from [1], we can draw the conclusion that MIESM gives better accuracy (in terms of r.m.s. error) than the others.

Fig. 8 and Fig. 9 show the difference of the BER calibration results from the MIESM algorithm in MCS1 and MCS10, using the configuration parameters shown in

Table 2. The scattered markers are the BER measurements obtained with multipath channel, while the solid line is the reference BER curve for AWGN channel.

The use of an analytical function to calculate the inverse Mutual Information would increase the calibration precision especially in lower modulation schemes where the experimental curves quickly increase towards asymptotic values (see Fig. 4), making difficult the estimation of the inverse Mutual Information needed in (1).

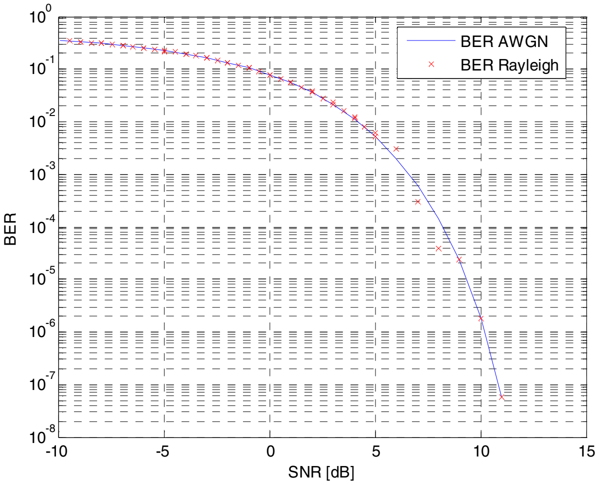


Fig. 8. MIESM Calibration Results for MCS1

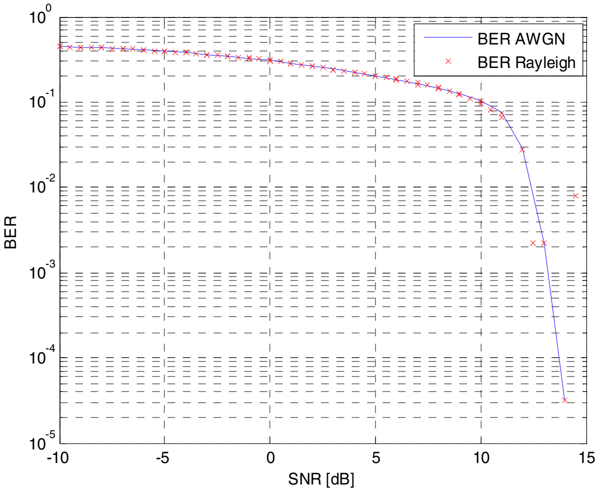


Fig. 9. MIESM Calibration Results for MCS10

5 Conclusions and Future Work

In this paper, the Mutual Information Effective SNR Mapping (MIESM) method for link-to-system mapping has been used in conjunction with an 802.16e link level simulator as a building block for a complete system level simulator. Simulations take into account the singularities of the 802.16e physical layer and important features of the MAC layer as well, such as H-ARQ, PUSC/FUSC and AMC. The results show that MIESM outperforms the other methods studied by us in [1]. The resulting calibration factor (β) brings the effective SNR curve closer to the reference AWGN curve, hence resulting in higher accuracy (lower r.m.s. error) than other methods. This holds especially for higher modulation schemes (large number of symbols). It is explained easily with the use of the equation described in (2).

Future work will continue studying realistic simulations using promising methods for link-to-system mapping such as weighted-training MIESM and Mean Mutual Information per Bit (MMIB) ESM. The use of an analytical function to calculate the inverse Mutual Information will also increase the calibration precision.

Acknowledgments. This research has been partially supported by the CELTIC ICARUS project “Distributed Wireless Networking Experimental Infrastructure for Optimization and Convergence” and funded by the Ministerio de Industria, Turismo y Comercio (TSI-020400-2008-113) of Spain.

We would like to thank Javier Lorca from the Radio Communication Group at Telefónica I+D for his support on the simulator used for this paper.

References

1. Aguilar, F.L., Cidre, G.R., López, J.M.L., París, J.R.: Effective SNR Mapping Algorithms for Link Prediction Model in 802.16e. In: International Conference on Ultra Modern Telecommunications & Workshops ICUMT 2009, pp. 1–6. IEEE, Los Alamitos (2009)
2. He, X., Niu, K., He, Z., Lin, J.: Link Layer Abstraction in MIMO-OFDM System. In: International Workshop on Cross Layer Design, IWCLD 2007, pp. 41–44. IEEE, Los Alamitos (2007)
3. Zhuang, J., Jalloul, L., Novak, R., Park, J.: IEEE 802.16m Evaluation Methodology Document (EMD). In: Srinivasan, R. (ed.) IEEE 802.16 Broadband Wireless Access Working Group. Intel Corporation (2009)
4. Mumtaz, S., Gameiro, A., Rodríguez, J.: EESM for IEEE 802.16e: WiMax. In: 7th IEEE/ACIS International Conference on Computer and Information Science, IEEE, Los Alamitos (2008)
5. Toumaala, E., Wang, H.: Effective SINR Approach of Link to System Mapping in OFDM/Multi-Carrier Mobile Network. In: 2nd International Conference on Mobile Technology, Applications and Systems, pp. 1–5. IEEE, Los Alamitos (2005)
6. Olmos, J., Serra, A., Ruiz, S., García-Lozano, M., Gonzalez, D.: Exponential Effective SIR Link Performance Model for LTE Downlink. European Cooperation in the Field of Scientific and Technical Research. Technical report, EURO-COST (2009)

7. 3GPP TS 36.104, Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) Radio Transmission and Reception (Release 8), v8.4.0. Technical specification, 3GPP (2008)
8. Bykovnikov, V.: The Advantages of SOFDMA for WiMAX. Technical report. Intel Corporation (2005)
9. Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems. Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands. IEEE Std. 802.16e-2005, IEEE (2005)
10. Guidelines for evaluation of radio interface technologies for IMT-Advanced, ITU-R M.2135, ITU (2008)

Virtual Distributed Simulation Platform for the Study and Optimization of Future Beyond 3G Heterogeneous Systems

Mª Carmen Lucas-Estañ[1], Salva Garrigas[2], Javier Gozálvez[1], Jose Monserrat[2],
Julen Maneros[3], Fernando López[4], Ainara González[5],
Imanol Aguado[1], and Pedro Chaparro[2]

[1] University Miguel Hernandez of Elche
[2] Polytechnic University of Valencia
[3] CBT Communication & Multimedia
[4] Telefonica I+D
[5] Innovalia Association
`m.lucas@umh.es, jomondel@iteam.upv.es,`
`jmaneros@cbt.es, fla@tid.es`

Abstract. This paper proposes and assesses a new distributed simulation platform for heterogeneous wireless communications. The objective of the ICARUS platform is to investigate cross-layer and cross-system algorithms for heterogeneous beyond 3G systems through a virtual distributed testbed that will allow the research community to share their individual simulation platforms and improve their research capacity through a cooperative simulation effort. This paper discusses the advantages of the ICARUS platform, and demonstrates its capacity to assess heterogeneous beyond 3G systems and reduce the simulation time.

Keywords: Distributed Simulation Platform, Beyond 3G Systems, Simulation Cluster.

1 Introduction

Technology evolution points to an always best connected wireless paradigm [1] with different technologies coexisting in the same area. The so-called seamless connectivity, and the resulting benefit for the user Quality of Experience (QoE), can be only accomplished through the coordination of the coexistent wireless technologies. This trend towards cooperation among heterogeneous Radio Access Technologies (RAT) is also known as beyond 3G communications. Its main goal is to serve each user with the RAT best-suited to the running application. The relevance of the concept of RATs cooperation in beyond 3G networks to improve the end user experience has been deeply studied in other European IST Projects, like Ambient Networks [2], Aroma [3] and Daidalos [4] with the common objective of improving the end user experience.

This complex heterogeneous framework requires an underlying architecture that allows users to be seamlessly served by different technologies. To this aim, the Common

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 368–379, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

Radio Resource Management (CRRM) entity should decide on which is the optimal network for each user and service demand, provided that users should be able to switch transparently from one RAT to another.

The challenging design of advanced CRRM algorithms raises the need of a heterogeneous simulation platform capable of adequately modeling the key aspects of heterogeneous beyond 3G wireless networks. The development of such heterogeneous platforms requires a significant development effort that can hardly be undertaken by individual research teams. In addition, the development of heterogeneous platforms by different teams duplicates development efforts and makes difficult a fair comparison of research proposals. It is also important to note that the emulation of various RATs in a single computer can significantly increase the simulation times and compromise the capacity to conduct high-impact research. To overcome this situation, several initiatives have been launched to develop virtual and distributed simulation platforms that allow the research community to efficiently share and run individual simulation clusters.

The WHYNET (Wireless Hybrid NETwork) project in the United States [5] and the Panlab (PAN european LABoratory infrastructure implementation) project in Europe [6] are key examples of research efforts to develop distributed simulation platforms. WHYNET is focused on the development of a scalable and distributed testbed for next generation mobile technologies, and its main aim is to study the cross-layer interactions. On the other hand, the main objective of PanLab is to create a federation of testbeds using the most innovative clusters in Europe.

In this context, this article presents an innovative distributed simulation platform for heterogeneous wireless technologies designed within the ICARUS project. The ICARUS platform is being designed to investigate advanced CRRM and RRM [7,8] policies for heterogeneous beyond 3G systems through the implementation of a virtual geographically distributed pan-european testbed. This testbed will allow the research community to share their individual RAT simulation platforms, and investigate advanced cross-layer and cross-system policies through an efficient, scalable and distribute platform. As a result, ICARUS is aligned with the objectives and procedures of Panlab.

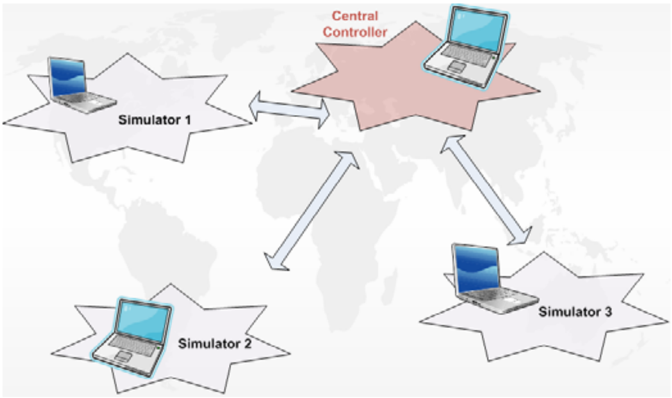


Fig. 1. Concept of the ICARUS virtual distributed simulation platform

The ICARUS network organization is shown in Fig. 1. The simulate RATs are emulated in different computers, which could be located in different locations. This architecture provides an important differential value to local platforms because of its flexibility and computational advantages. The ICARUS platform is expected to achieve faster simulation times through the use of distributed computational resources, and reduce the implementation load by sharing the use of different simulators that can be easily shared thanks to the modular and scalable design of the platform. In this context, the ICARUS platform will provide a valuable environment for testing advanced cross-layer and cross-system optimization algorithms that will be key for an efficient deployment and operation of heterogeneous beyond 3G systems.

2 ICARUS Platform

The ICARUS project is aimed at providing a virtual distributed platform for the emulation of a heterogeneous mobile and wireless communication system. In this context, the different RATs considered within the ICARUS platform could be implemented in different simulators independently developed and running on physically distributed computers. To ensure that all these independent simulators are integrated to synchronously emulate the same scenario through a virtual and distributed simulation platform, different functionalities must be implemented at a common level to carry out the global management of some scenario simulation aspects. Fig. 2 illustrates the different management levels considered within the ICARUS Virtual Distributed Testbed (VDT). These management levels are:

- Common Management Level. To be able to emulate a unique common scenario, functions that need to work globally are located at this management level. These common functions are implemented externally to all the simulators. The main entity in the Common Management Level is the Central Controller. This entity manages the information exchange between software simulators and common management functional modules. All the entities located at the Common Management Level will make up the so-called VDT-Controller (VDT-C). It is not mandatory to implement all the common functionalities included in the VDT-C in the same computer. They can be distributed in different computers and remotely connected to the platform to ensure the maximum flexibility and extendibility.

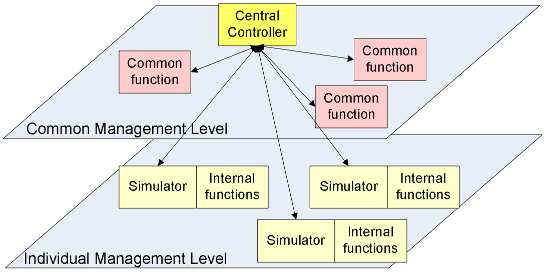


Fig. 2. ICARUS platform functional levels

- Individual Management Level. The functions located at this level are implemented within each simulator, and will individually manage specific functions for each of the simulators implemented and run remotely.

To identify which functions must be implemented at the common functional level, two objectives have to be considered. The first one is to minimize the information exchange between remote simulators or functional modules integrating the ICARUS platform since a constant exchange of messages through the Internet will increase the execution times. In addition, to facilitate the integration of individual simulation clusters within ICARUS, the number of modifications in these platforms should be minimized. In this context, the main identified functions that need to be implemented at the common management level are: CRRM, Session and Traffic Generation, and Mobility Management.

The interaction between the remote modules (simulators and common functional modules) composing the ICARUS platform will be made through the exchange of signalling messages. However, the different modules composing the platform will be only able to communicate with and through the Central Controller (see Fig.2). In this context, the Central Controller is in charge of managing all the messages exchanged in the ICARUS platform: all the messages are sent to the Central Controller which interprets the received messages, and creates and sends the necessary messages to the targeted modules. For example, if a user assigned to a given RAT needs to know the channel quality of other RATs at a given time, the current RAT will demand this information to the Central Controller which will ask this information to the other RATs implemented in different simulators.

To illustrate the potential and benefits of the ICARUS platform, a simple scenario has been initially considered. This first scenario considers a heterogeneous system composed by the EDGE (Enhanced Data-rates for GSM/Global Evolution) and HSDPA (High Speed Downlink Packet Access) RATs. These RATs are emulated by two different applications of the SPHERE (Simulation Platform for HEterogeneous wiREless systems) simulator [9] located in two different computers. A third computer implements the VDT-C to manage and run advanced cross-layer and cross-system studies through the ICARUS distributed testbed. The SPHERE platform, the VDT-C and the mechanisms to carry out the remote interaction between modules are described in following subsections.

2.1 SPHERE Platform

SPHERE (Simulation Platform for HEterogeneous wiREless systems) is a novel, ambitious and scalable radio simulation platform for heterogeneous wireless systems initially developed by the University Miguel Hernandez of Elche, and subsequently jointly developed together with the Polytechnic University of Valencia [9]. The platform currently integrates four advanced system level simulators, emulating the GPRS (General Packet Radio Service), EDGE, HSDPA and WLAN Radio Access Technologies (RATs). SPHERE is a unique discrete-event system level simulation platform that emulates all four RATs in parallel at the packet level, which enables an accurate evaluation of the final user perceived QoS through the implementation of novel CRRM and RRM mechanisms. The radio interface specifications [10,11] of these four technologies have been faithfully implemented in the SPHERE simulation platform, which works with a high time resolution (in the order of some milliseconds). This modeling approach guarantees the capability of the SPHERE simulation platform to dynamically and precisely evaluate the performance of RRM/CRRM techniques.

Fig. 3 shows the scenario modeled by the SPHERE platform which includes the GPRS, EDGE, HSDPA and WLAN radio interfaces and concentrates on the downlink. As shown in Fig. 3, the SPHERE platform does not only model the radio interface of the four technologies, but also implements various RAT specific RRM features and a centralized CRRM entity. This entity directly collects specific RAT information (e.g. load, channel quality conditions, etc) and interacts with the RRM entities of each RAT. The logical structure of the SPHERE simulation platform is also shown in Fig. 4. This figure depicts the modular and scalable design of the platform [9], which guarantees an easy adaptation of the platform configuration to specific requirements, and allows the rapid integration of new functionalities.

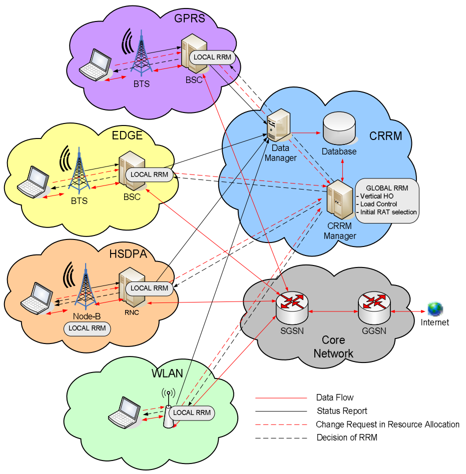


Fig. 3. SPHERE heterogeneous scenario

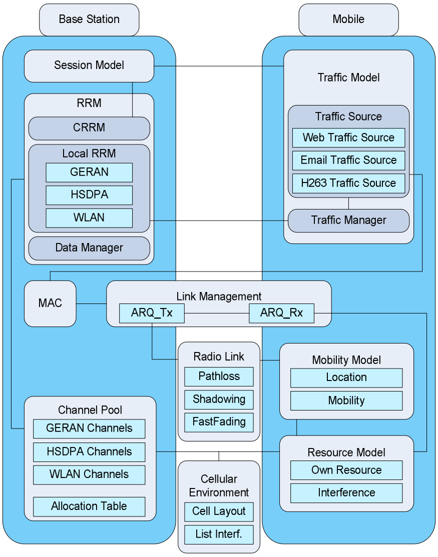


Fig. 4. SPHERE logical structure

2.2 SPHERE Adaptation to the ICARUS Platform

As shown in Fig. 4, the initial SPHERE simulator incorporates all the functionalities that have to be located in the Common Management Level in the ICARUS platform. For example, the SPHERE platform incorporates its own Session and Traffic Sources (see Fig. 4). As previously explained, the session and traffic generation needs to be implemented as global and common functions to all the simulators that compose the ICARUS platform. As a result, the Session and Traffic Sources have been disabled in the SPHERE simulator, and have been relocated in the VDT-C at the common management level. In this case, each time a new session is generated, all the information regarding the traffic session (session start time, session duration, service type, number of traffic objects to transmit, size of the traffic objects, etc.) is created in the VDT-C. This information is then sent to the distributed SPHERE simulators that store the traffic information in the User Context, a new module created to store the information related to the user traffic session sent by the VDT-C. To emulate the transmission of the traffic session, the SPHERE Traffic Manager will read the User Context information associated to the corresponding user and will create all the related traffic events. The adapted logical structure of the SPHERE simulator to interact with the VDT-C in a distributed manner is depicted in Fig. 5. This figure shows that the CRRM entity has also been disabled in SPHERE and located in the Common Management level. In the ICARUS platform, the CRRM decisions are taken at the VDT-C; the VDT-C is the more suitable location given that it can communicate directly with all the simulators composing the platform. In this regard, each time a new user requests access to the system, the CRRM entity located at the Common Management Level will take the CRRM decision, as for example, to select the RAT over which to convey the user session among all available RATs emulated in the ICARUS platform. Then, the VDT-C will communicate the corresponding simulator that a new user is assigned to the selected RAT. The simulator will still be in charge of performing RRM functions within each RAT.

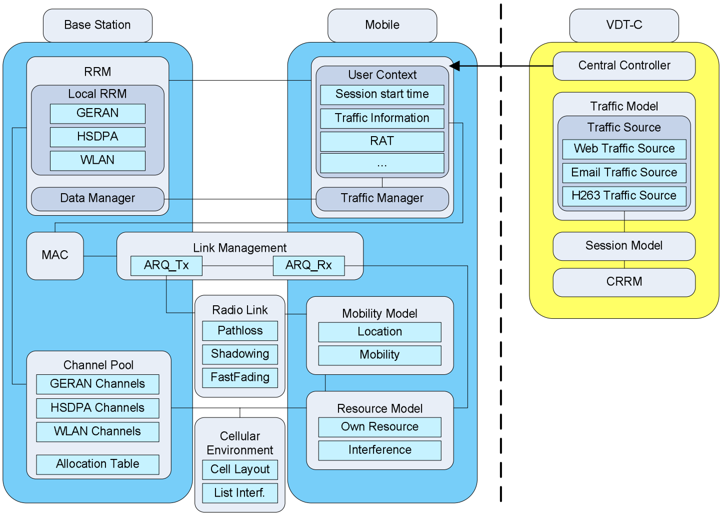


Fig. 5. SPHERE logical structure adapted to the ICARUS platform

2.3 VDT-C

Fig. 5 shows the logical structure of the implemented VDT-C. The main entity of the VDT-C is the Central Controller which is in charge of the management of the information exchange between the different modules. The Central Controller is also responsible of the whole platform synchronization. Due to the fact that each simulator might run at different speeds, synchronization points to carry out the communication among the different modules have to be established. Otherwise, a simulator could send an event with an execution time previous to the current simulation time of the destination simulator, and then a conflict would take place. In the ICARUS platform, these synchronization points are referred as Time Steps and are periodically scheduled. When a simulator reaches a Time Step, it notifies the Central Controller of this fact. Then the simulator pauses its simulation process waiting for the other simulators, and no new events will be exchanged among different modules until all simulators notify that they have reached the same Time Step. When the Central Controller knows that all simulators are at the same Time Step, it asks the simulators for new messages. When all the messages have been sent and processed, the Central Controller orders the simulators to resume their simulation until the next Time Step.

The other common functionalities that are currently implemented in the ICARUS VDT-C are the Session and Traffic Sources and the CRRM entity. The session and traffic models implemented in the VDT-C are those considered in the initial SPHERE simulator, and a short description was given in Section 2.1. On the other hand, the CRRM entity is in charge of the common management of the total available radio resource in the system. In the introduction of this section, the Mobility Management was also identified as a necessary global functionality. The global Mobility Management becomes really necessary when handovers between RATs implemented in different simulators are considered. When a user is handed over to a different RAT, the new RAT must be able to carry on with the user movement without abrupt direction changes and jumps. In this case, a global management of the user movement is needed. Since the initial scenario that has been used to validate the ICARUS platform considers a simple initial RAT selection policy without vertical handovers, the mobility model is kept at the SPHERE simulators. The authors are currently working to migrate this model to the VDT-C for more advanced CRRM studies.

2.4 Remote Communications

The communications and exchange of information among remote modules and simulators has to be made over the Internet. In this regard, sockets have been employed to carry out this remote communications and correctly control the exchange of data. To establish the communications, each simulator and functional module has to implement an API (Application Programming Interface) that implements all the functions related with the sockets management and exchange of information. This API can be written in different programming languages based on the simulator or functional module it is integrated with. In addition, a gateway needs to be implemented for each remote module to interpret the exchanged information, and adapt it to the format required by the local simulator or functional module. The communications between remote modules has been implemented as a Client-Server interaction as shown Fig. 6. In this context, the VDT-C is always listening for messages, while the distributed simulators send messages to the VDT-C and then wait for answers.

In the current implementation, all the common functionalities located in the VDT-C have been implemented in the same computer. As a result, only the messages needed for the communications of the remote simulators with the VDT-C have been defined:

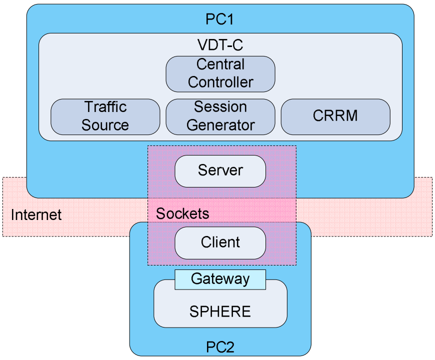


Fig. 6. ICARUS interaction among remote modules

- *Initial configuration* message (*ic*). This message is sent by the Central Controller before the simulation itself starts, and allows each simulator to load the needed configuration parameters.
- *Add user* message (*au*). This message is sent by the Central Controller to one of the distributed simulators when a user needs to start a service session using the RAT associated to that simulator. With this message, the controller provides the simulator with the needed information regarding the user and the type of service required.
- *End simulation period* message (*ep*). This message is sent by each simulator to the Central Controller when a Time Step is achieved, i.e, a simulation period is finished. The simulator includes in this message information regarding the users and RAT status.
- *Resume simulation* message (*sr*). After the exchange of information between remote nodes at a given Time Step, the VDT-C sends the resume simulation message to all the distributed simulators, so that they continue their simulation until the next Time Step.
- *End simulation* message (*es*). This message is sent by each simulator to the Central Controller at the end of the complete simulation.
- *ACK* message. To guarantee the robustness of the distributed ICARUS platform, all the exchanged messages have to be confirmed, which is the role of the ACK messages. All the messages sent through the network have related a timeout. If the ACK message is not received before the timeout expires, the message is re-sent.

3 Use Case Implementation and Performance

To test and validate the first version of the ICARUS platform, as well as the adaptations carried out on SPHERE, a first evaluation scenario has been proposed. In this first scenario, a heterogeneous system only composed by the RATs EDGE and HSDPA is considered. Both RATs are emulated by two different applications of the SPHERE simulator in two different computers, and the VDT-C is also located in a third computer. In this scenario, only the initial RAT selection dilemma is considered and vertical handovers have not been implemented. This simple CRRM policy will assign the user to the RAT corresponding to the demanded service based on a predefined relationship RAT-service type [12]. In this scenario, email users will be assigned to EDGE, while web transmissions will be conveyed over HSDPA.

Fig. 7 shows the flowchart of the simulation process in both the simulators and the VDT-C. At the beginning of the simulation, the SPHERE simulators and the VDT-C read the configuration parameters from the configuration file (*ic* message). Then, the SPHERE simulators send to the Central Controller the *ep*[1] message indicating that it has reached the first Time Step (synchronization point), and wait for new events from the Central Controller. The Central Controller waits to receive the *ep* message from all the active SPHERE simulators. When this happens, the Central Controller asks the Session Source if new sessions have arrived, and if this is the case, the new sessions are assigned to users and the traffic related to each session is created. The CRRM algorithm is then executed and the RAT to which each user will be assigned is decided. At this moment, the Central Controller sends the *au* message to inform the corresponding simulators that new users are assigned to the RAT they are emulating. When the corresponding simulator receives the *au* message, it processes the event and stores in the User Context of each new user the traffic session information sent in the

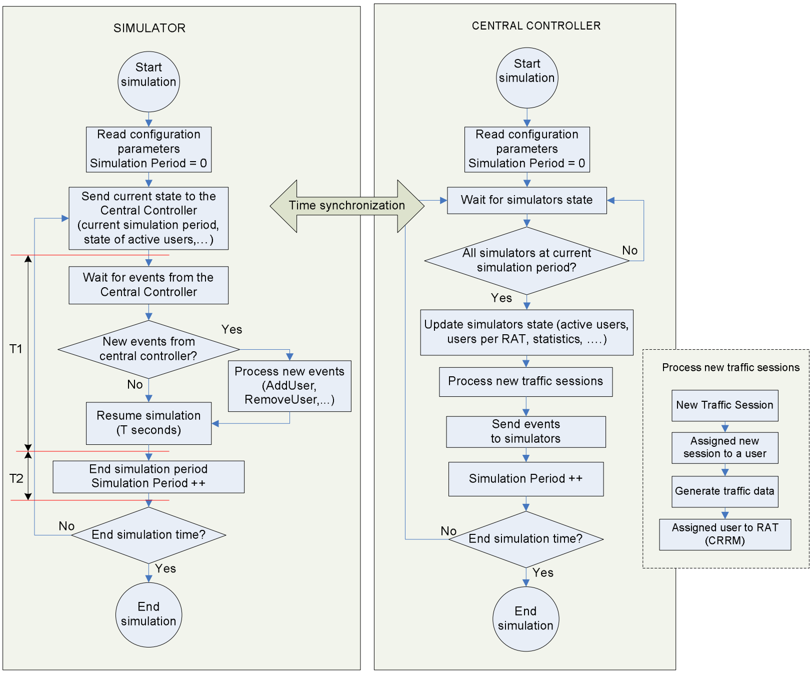

SIMULATOR
Start simulation
Read configuration parameters Simulation Period = 0
Send current state to the Central Controller (current simulation period, state of active users,...)
Wait for events from the Central Controller
T1
New events from central controller?
Yes
No
Process new events (AddUser, RemoveUser,...)
Resume simulation (T seconds)
T2
End simulation period Simulation Period ++
No
End simulation time?
Yes
End simulation
Time synchronization
CENTRAL CONTROLLER
Start simulation
Read configuration parameters Simulation Period = 0
Wait for simulators state
All simulators at current simulation period?
No
Yes
Update simulators state (active users, users per RAT, statistics, ...)
Process new traffic sessions
Send events to simulators
Simulation Period ++
No
End simulation time?
Yes
End simulation
Process new traffic sessions
New Traffic Session
Assigned new session to a user
Generate traffic data
Assigned user to RAT (CRRM)

Fig. 7. ICARUS simulation process

---

[1] All the messages sent over the network are acknowledged through an ACK message.

au message. Based on this traffic session information, events are created in the RAT simulator to emulate the session transmission. The simulator waits for more events until receiving the *sr* message indicating to resume the simulation until the next Time Step, i.e., for another simulation period. The *sr* message is sent by the Central Controller when it has processed all its events and the corresponding messages have been sent to the simulators. After sending the *sr* message, the Central Controller runs until the next Time Step and waits for the simulators to conclude the current simulation period. If a user ends the traffic session transmission, the RAT simulator will inform the VDT-C in the next *ep* message and send the corresponding transmission statistics.

Table 1 summarises the ICARUS platform's configuration. The ICARUS platform emulates a 27 omnidirectional cellular layout, with 500m radius cells offering EDGE and HSDPA coverage. Base stations for both RATs are co-located in the centre of a cell. Each simulated RAT has been assigned a single frequency carrier per cell, which results in eight channels, or timeslots, for EDGE, and fifteen channels, or codes, for HSDPA. A multimedia traffic environment with email and web users is emulated with a session arrival rate of 0.08 and 0.09 sessions per second respectively.

To validate the capability of the distributed ICARUS platform to accurately investigate CRRM techniques, the performance achieved with the ICARUS testbed has been compared to that achieved with a single SPHERE platform emulating simultaneously and in a single computer the EDGE and HSDPA RATs. This comparison will allow identifying the expected benefits and trade-offs in terms of simulation time and results accuracy. Fig. 8 depicts the performance results in terms of BLER (Block Error Rate) and throughput obtained when simulating the described scenario in the distributed ICARUS platform, or in a single computer simultaneously emulating the EDGE and HSDPA RATs. Different simulation periods (time between two consecutive Time Steps) have been configured in the ICARUS platform to evaluate the negative effects that this parameter can introduce in the simulator's performance accuracy. Fig. 8 shows that the results obtained with both simulation approaches are very similar irrespectively of the considered Time steps[2].

The execution time need to simulate a 30000s emulation is shown in Table 2. The results show that the execution time is reduced using the ICARUS distributed platform compared to when simulating in parallel and in the same computer different RATs using the SPHERE platform. Moreover, the execution time is reduced as the simulation period between two consecutive Time Step increases. However, although increasing the simulation period has not had negative effects on the performance of the scenario emulated in this work, this parameter will be actually critical when vertical handovers are considered. If the CRRM decision is not taken in a short time when a user requests a handover, for example due to low signal level, the user call could be dropped. In this context, a tradeoff between performance reliability and computation feasibility and cost will have to be achieved. Table 3[3] shows the measured T1 and T2 times depicted in Fig. 7 for each one of the simulators currently composing the distributed ICARUS platform. T1 corresponds to the time spent exchanging messages with the VDT-C, while T2 is the time that the simulator actually spends emulating a new simulation period equal to the Time Step. The obtained results show that the

---

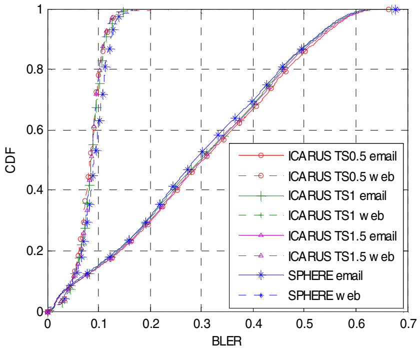
[2] Despite these results, a performance difference is expected for higher Time Steps.

[3] Both simulators run in identical computers (Intel Dual-Core Xeon 3 GHz FSB 667MHz).

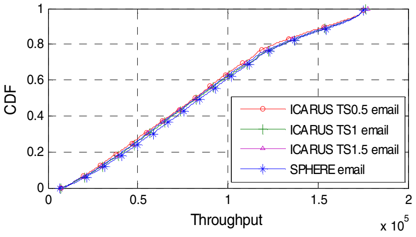
Table 1. ICARUS configuration parameters

Parameter	Value	Parameter	Value
Simulated cells	27 omnidirectional cells	Mobility	3 km/h user speed
Environment	Macrocellular urban scenario	Pathloss	Okumura-Hata COST 231 Hata
Cellular radio	500 meters	Shadowing	Log-normal with 6dB standard deviation
Channels per cell	8 EDGE channels, 16 HSDPA channels		
Users per cell	30 users	Session arrival rates	Email: 0.08 sessions/s Web: 0.09 sessions/s

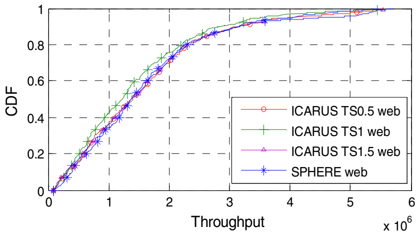
exchange of information with the VDT-C only corresponds to the 12.78% of the total execution time, which is not that significant compared to the high computational requirements of the HSDPA simulator.



a) BLER for email and web users



b) Throughput for email users



c) Throughput for web users

Fig. 8. Performance results

Table 2. Execution time for a 30000s emulation

	Execution time	Improvement (%)
SPHERE	62987s	-
ICARUS Time Step 0.5s	55696s	11.58
ICARUS Time Step 1s	47879s	23.99
ICARUS Time Step 1.5s	46183s	26.68

Table 3. Execution times of the ICARUS simulators for a 1 second Time Step

	T1	T2
EDGE simulator	0.949s	0.647s
HSDPA simulator	0.204s	1.392s

4 Conclusion

This work has presented a first successful implementation of a distributed platform for future beyond 3G heterogeneous wireless systems developed in the framework of the ICARUS project. The distributed approach allows interconnecting and collaboratively sharing simulation platforms developed by different groups for a more resource and performance efficient research on complex issues of Beyond 3G systems. To this aim, some common functionalities and interfaces between the different platforms have been identified and implemented in a control entity named VDT-C. To validate the distributed and cooperative simulation approach proposed in ICARUS, this paper has implemented a simple CRRM policy. The results obtained have initially validated the capacity of the ICARUS platform for cross-layer and cross-system studies in Beyond 3G scenarios. In addition, a gain in execution times with the distributed platform has also been highlighted.

Acknowledgement

This work has been supported by the Spanish Ministry of Industry, Tourism and Trade under the ICARUS project TSI-020400-2008-113 (Celtic proposal CP5-013).

References

1. Gustafsson, E., Jonsson, A.: Always best connected. In: IEEE Wireless Communications, vol. 10, no. 1, pp. 49-55, (2003)
2. IST-Ambient Networks Project AN-R6.1: Network Context Management: Concepts, Scenarios and Analysis of State of the Art, https://bscw.ambient-networks.org/bscw/bscw.cgi/0/7743 (2004)
3. IST-AROMA Project D09: First report on AROMA algorithms and simulation results, http://www.aroma-ist.upc.edu (2006)
4. IST-Daidalos Project D321: QoS Architecture and Protocol Design Specification, http://www.istdaidalos.org (2004)
5. The WHYNET project, http://pcl.cs.ucla.edu/projects/whynet
6. The Panlab project, http://www.panlab.net
7. Sallent, O.: A Perspective on Radio Resource Management in B3G. In: 3rd International Symposium on Wireless Communication Systems (ISWCS'2006), pp.30-34, Valencia (Spain) (2006)
8. Gozalvez, J., Gonzalez-Delicado, J.J.: CRRM Strategies for Improving User QoS in Multimedia Heterogeneous Wireless Networks. In: 20th IEEE Personal, Indoor and Mobile Radio Communications Symposium (PIMRC'09), Tokyo (Japan) (2009)
9. Gozálvez, J., Martín-Sacristán, D., Lucas-Estañ, M., Monserrat, J.F., González-Delicado, J.J., Gozalvez, D., Marhuenda, M.: SPHERE- A Simulation Platform for Heterogeneous Wireless Systems. In: 3rd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom), pp. 1-10, Orlando (Florida) (2007)
10. 3GPP, Technical Specification Group GSM/EDGE Radio Access Network; General Packet Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2, 3GPP TS 43.064, version 6.3.0 (2004)
11. 3GPP, Radio Interface Protocol Architecture, 3GPP TS 25.301, version 6.4.0 (2005)
12. Pérez-Romero, J., Sallent, O., Agustí, R.: Policy-based Initial RAT Selection algorithms in Heterogeneous Networks. In: 7th Mobile and Wireless Communications Networks Conference (MWCN), pp. 1-5, Marrakesh (2005)

A Dual Head Clustering Mechanism for Energy Efficient WSNs

Muhammad Alam and Jonathan Rodriguez

Instituto de Telecomunicações
Universitário de Santiago Aveiro
P-3810-193 AVEIRO, PORTUGAL
{alam,jonathan}@av.it.pt

Abstract. Wireless sensor network are resource constrained. Clustering techniques are used to conserve energy and to prolong the lifetime of the wireless sensor network. A number of clustering techniques have been presented based on single cluster head. In single cluster head mechanisms, the single cluster head is responsible for both data gathering and data forwarding so it consumes more energy compared to the other member nodes and dies earlier. In this paper we propose a Dual Head Clustering Mechanism (DHCM) for wireless sensor network. The DHCM is based on two cluster head, one cluster head selects the data and the other head is responsible for data forwarding set for a specified number of rounds. The simulation results show that the DHCM reduce the overhead over a single head and improves the life time of the network.

1 Introduction

The current development in micro-sensor networks has made it feasible to manufacture very small sensor devices. Wireless sensor network can be made by connecting a large number of sensor nodes. The network formed by these sensor nodes depends upon the area or events to monitor and the proposed application domain for which the wireless sensor network is developed. Usually these sensors are unattended, immovable and energy constrained. Once these nodes are deployed, they start sensing the environment, make computations and disseminate this information to the base station [1, 2, 3]. The base station is normally stationary (can be mobile as well) and energy sufficient. Each sensor node is specified with a specific task or mission and can gather context information using available computational power, energy and bandwidth. A typical wireless sensor network is shown in the figure 1. Wireless sensor networks have a large number of applications which includes military, weather monitoring, tactical surveillance, distributed computing, security, habitat monitoring, detecting events such as moments, temperature, sound, industrial manufacturing [4] etc.

Cluster routing has been introduced to reduce the energy usage in routing. In cluster routing all nodes in the network organize themselves in form of clusters (or groups). There are usually three steps involved in clustering algorithms. In the first phase the cluster head (CH) is selected in a cluster and this information is disseminated to all the nodes in the cluster. Member nodes also inform the cluster head (CH)

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 380–387, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

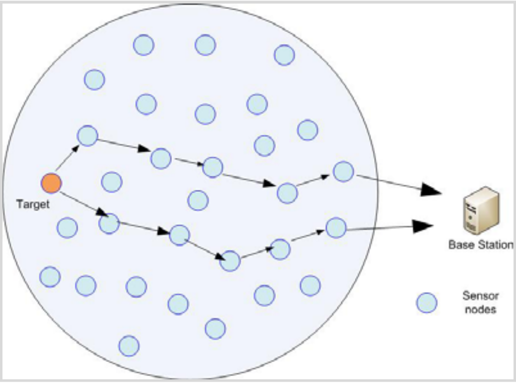


Fig. 1. Wireless Sensor Network

about their presence in the cluster. In the second phase all the member nodes sense the environment, collect the data and communicate with their cluster heads alone. In the third and last phase the cluster heads aggregates all the collected information and sends it to the base station either directly or by using multi-hop routing as in figure 2. Whichever WSN mechanisms are in place, they must have desirable attributes that include to be power aware, capable of optimum routing, adaptive, reliable, scalable and fault tolerant.

In this paper we propose a Dual Head Clustering Mechanism (DHCM). The communication between the cluster head and the sink is multi-hop. There are still challenges with the multi-hop routing as the cluster head close to the base station dies earlier, an issue that was attempted to be resolved by Energy Efficient Unequal Clustering (EEUC); however there is still burden on the cluster head. Unlike other previously proposed algorithms, we have taken two cluster nodes as cluster heads with different responsibilities and have compared their performance which is further elaborated in section 4 and section 5.

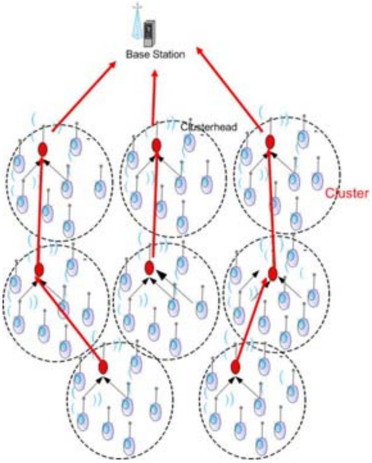


Fig. 2. Cluster based wireless sensor network

The rest of this paper is organized as follows: section 2 presents related work; section 3 describes the network model; in section 4 our algorithm is presented; section 5 presents the simulation parameters and results, and section 6 gives the conclusions and future work.

2 Related Work

A number of clustering techniques have been introduced all focusing on saving energy and thus increasing the overall lifetime of wireless sensor networks. Brief descriptions of some of the proposed clustering mechanisms are presented here.

Heinzelman, et al. [5] introduced a clustering algorithm for sensor networks, called Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH solves the problem of static clustering mechanisms in which the cluster heads, once selected, will remain assigned throughout the lifetime of network. LEACH selects a few sensor nodes as cluster heads and rotates the role of cluster heads depending upon the energy of the nodes. The operation of LEACH consists of two phases, the setup phase and the steady state phase. In the setup phase, the clusters are organized and cluster heads are selected. Only 5 % of nodes are selected as cluster heads. During the steady state phase, the sensor nodes begin sensing the environment and collect data and then transmit this data to the cluster heads. The cluster head aggregates the received data and sends it to the base station. In [6], an enhancement over the LEACH protocol was proposed. The protocol is called Power-Efficient Gathering in Sensor Information Systems (PEGASIS). In PEGASIS nodes do not communicate directly with the base station, instead they communicate with their closest neighbours which in turn communicate with the BS. Thus PEGASIS extends the lifetime of network. To locate the closest neighbor node in PEGASIS, each node uses the signal strength to measure the distance to all neighboring nodes and then adjusts the signal strength so that only one node can be heard. The aggregated data is sent to the sink by any node in the chain. The Simulation results show that PEGASIS is able to increase the lifetime of the network to twice that of the LEACH protocol. An extension to PEGASIS, called Hierarchical PEGASIS, was introduced in [7]. The main objective of Hierarchical PEGASIS is to decrease the delay incurred for packets during transmission to the sink. Results shows that that Hierarchical PEGASIS perform better than the regular PEGASIS scheme by a factor of about 60. In [8] Energy Efficient Clustering Scheme (EECS) a new approach has been introduced. EEUC is hierarchal clustering algorithm that partitions the nodes into clusters of unequal size, and clusters closer to the base station have smaller sizes than those further away from the base station. With this scheme cluster heads closer to the base station will save energy for the inter-cluster data forwarding. EEUC is a distributed competitive algorithm and with no iteration so EEUC is different from LEACH and HEED. The node's competition range to become cluster head decreases as its distance to the base station decrease. In the proposed multi-hop routing protocol for inter-cluster communication, a cluster head chooses a relay node from its adjacent cluster heads according to the node's residual energy and its distance to the base station. The simulation results presented shows that EEUC performs better than LEACH and HEED. To improve EEUC Energy-Efficient Level based and Time-based Clustering (EELTC) have been introduced in [9].

EELTC is hierarchical clustering algorithm and has the ability of creating unequal clusters with very low controlling overhead. In EELTC all sensors determine their level by receiving a message from the base station. The main idea is the optimal selection of CHs based on their level and residual energy. The number of clusters formed near the base station is less in number than the number of clusters formed away from the base station. The proposed mechanism has then been compared with the previous existing LEACH and EEUC. The results show that EELTC saves more energy in setup phase since it has lower message overhead than LEACH AND EEUC.

3 Network Model

We consider N sensors in our network and make the following assumptions.

- All sensors have equal significance.
- The base station and all the sensor nodes are stationary after the network is deployed and the base station is located far from the sensor field.
- All the sensors are location aware and not equipped with GPS and are capable to compute the distance by signal strength.
- All the sensor nodes have a unique ID.
- The Data cluster head is responsible to aggregate the data packets received from the members' nodes and hand over to the routing cluster head. The routing cluster head receives data from other clusters.

We have used a simplified energy model used in [8, 9], which has been used in most of the previous related work. The d^2 power loss model is used if the distance d between transmitter and receiver is less than the threshold $d_0$otherwise d^4 power loss model is used, so in order to transmit k-bits massage over distance d the electrical energy is given by:

$$E_s\,(k\,,d) = \begin{cases} k.E_{elec} + k.\varepsilon_{fs}.d^2 & d < d_0 \\ k.E_{elec} + k.\varepsilon_{mp}.d^4 & d \geq d_0 \end{cases} \tag{1}$$

Where E_{elec} denotes the electrical energy; and the ε_{fs} and ε_{mp} are the amplifier energy.

To receive a massage k the energy spent is given by the following equation.

$$E_r\,(k\,) = k\,.E_{elec} \tag{2}$$

For fusion: if we have n massages and each with k-bits, the energy is:

$$E_f\,(m\,,k) = m\,.k\,.E_{fuse} \tag{3}$$

4 DHCM Approach

The DHCM has three phases: cluster setup, multi-hop routing formation and data transmission. The DHCM is based on rounds, but unlike other algorithms the setup phase remains the same for some specified number of rounds. Let's suppose x is the number of rounds for which the setup phase will restart. If the initial value of x is 10 then it means that after 10 rounds the setup phase will restart and new heads will be selected. This x value will be decreased as time passes and will eventually reach 1. Thus with this method we can save the energy that is consumed in the setup phase in the early life time of network. Initially the value of x is high because all the nodes have high energy and this level decreases when they start their operations. We have used the dual cluster heads because with single cluster head a considerable amount of energy is consumed in each round and we may not be able to fix the same cluster head for a specified number of rounds.

4.1 Cluster Setup

When the network is deployed the base station sends a broadcast message to all the sensor nodes at a certain power level. Based on the received signal strength each node then computes its approximate distance d to the base station. This distance d calculation is used in the calculation of the radius for the cluster. Let R_{max} be the maximum value for the radius, R_{min} be the minimum value for the cluster and d_j is the distance of node j from the base station: then we define the cluster size of node j as

$$R_j = \frac{d_j \cdot (R_{\max} - R_{min})}{d_{max}} + R_{min} \tag{4}$$

Once the cluster radius is specified and each node knows its cluster then each node broadcasts a *HELLO* massage which has the *id* and energy of the node. Each node receives a broadcast massage and saves this information. Then based on the information on each node the node j is elected as Data Cluster Head (DCH). Once a node is selected as DCH it broadcast an information massage to all nodes. Each node in the radius then computes its distance to the DCH and if it is less than R_j it considers node j as cluster head and saves the information. Once the DCH is selected the next step is to elects the Routing Cluster Head (RCH). The node with highest energy and minimum distance to the DCH is selected as the RCH.

4.2 Inter-Cluster Multi-hop Routing

Hierarchal routing is one of the best routing techniques used for energy conservation in wireless sensor network and hence adopted in this network. After the setup phase the RCH, which is responsible for routing, broadcasts a message to the RCHs electives of other clusters. This broadcast massage contains the id, energy level and the distance from the base station. On receiving the broadcast massage, each RCH computes the distance to the other RCH and selects the shortest route to the base station. This route selection is also restricted by the number of rounds value.

4.3 Data Transmission

In the data transmission phase each member node in the cluster starts sensing the data and sends it to the DCH. The DCH on receiving the data, aggregates it, and send it to the RCH. The RCH, on receiving the data from other clusters, forwards the data to the base station. Due to short DCH-RCH distance, less energy is consumed by the DCH in the data transmission phase. Furthermore, each RCH has the option to select short but high energy paths to forward the data to the base station.

5 Simulation Results

This section presents the performance evaluation of DHCM via simulations. We assume an ideal MAC layer and error free communication link for this simulation. We run extensive experiments and the results presented here are the average of all those simulation results. The parameters used in the simulation are listed in table1. We have compared DHCM with the previously proposed LEACH and EEUC algorithms.

Table 1. Simulation Parameters

Parameters	**Value**
Area	200 x 200
Location of Base station	100, 350 m
Algorithms used	LEACH, EEUC,DHCM
Number of Sensors	200
Initial energy	4J
E_{elec}	50nJ/bit
ε_{fs}	10pJ/bit/m^2
ε_{mp}	0.0013pJ/bit/m^4
E_{fuse}	5nJ/bit/signal
Packet size	4000 bits
d_0	87 m
R_{max}	70 m
R_{min}	30 m

5.1 Energy Consumpton of Cluster Heads

The calculation of energy consumption by the cluster heads in 40 rounds are shown in the figure 3. In LEACH the data is directly sent to the base station by the cluster heads so the energy consumption is very high. In EEUC and DHCM, multi-hop communication is used to forward the data from the cluster heads to the base station, so due to the small distances between the cluster heads compared to the direct distance to the base station, a considerable amount of energy is saved. We have considered the combined energy consumption by both cluster heads. Furthermore, the energy consumption of DHCM is lower than EEUC beacuse the EEUC consumes energy during the setup phase of each round, while the DHCM uses the same set of clusters for a specified number of rounds.

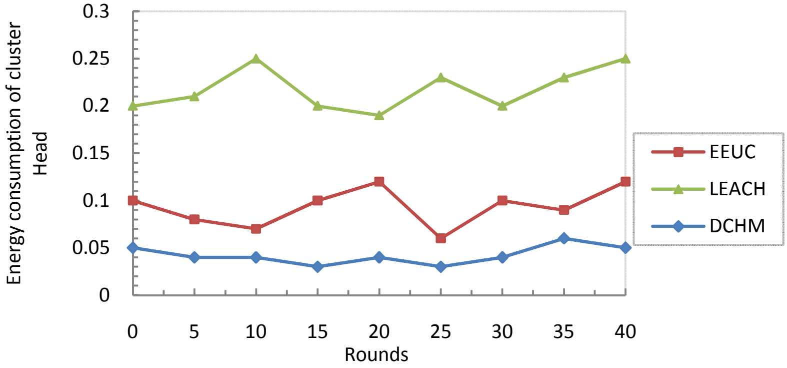


Fig. 3. Energy consumption of cluster heads

5.2 Network Life Time

DHCM improves the lifetime of the network in terms of the amount of time until the first and last node die as shown by figure 4. Due to single-hop routing, the node dies earlier in the LEACH protocol as the nodes further away from the base station consume more energy to send data directly to base station. By using multi-hop routing in EEUC the network lifetime significantly increases over LEACH. Moreover, as in DHCM the heads are set for a specified number of rounds so a considerable amount of energy is saved and this improves the overall network life time e.g. if we set the value for the number of rounds to be 5, this means new cluster heads will be selected after 5th round and thus we can save the setup phase energy consumption 5 rounds. Due to the above mechanism, DHCM outperforms LEACH and EEUC.

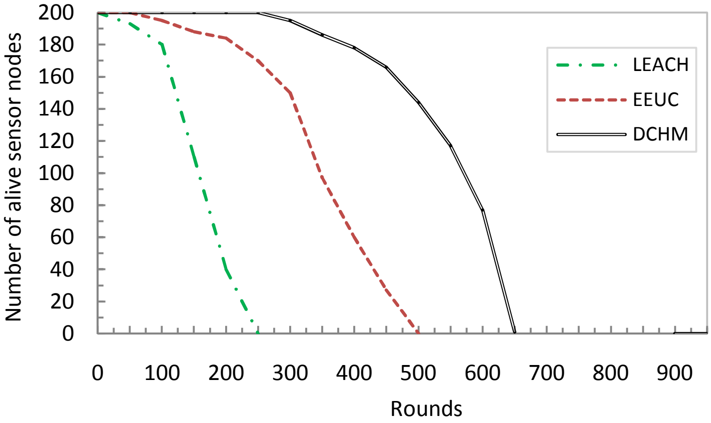


Fig. 4. The number of alive sensor nodes

6 Conclusions

In this paper we have presented a novel energy aware multi-hop cluster routing protocol for WSN called DHCM. DHCM has two cluster heads; one is responsible for the data gathering and the other for data forwarding. In the cluster setup phase, the cluster heads are set for a specified number of rounds and this value decreases with time. The simulations results have shown that the DHCM outperforms the LEACH and EEUC, and significantly increases the network lifetime.

Acknowledgments. The work presented in this paper has been performed in the framework of the ICT-PEACE project (contract no. 225654) funded by the European Union.

References

1. Pottie, G.J., Kaiser, W.L.: Wireless integrated networks sensors. Communication of the ACM 43(5), 51–58 (2000)
2. Li, Q., Aslam, L., Rus, D.: Hierarchical powr-aware routing in Sensor nehvorks. In: DIMACS Workhop on Pervasive Networking (May 2001)
3. Intanagonwiwat, C., Govindan, R., Estrin, D.: Directed diffusion: a scalable and robust communication paradigm for sensor networks. In: Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000) (August 2000)
4. Shah, R.C., Rabaey, J.: Energy aware Routing for low Energy ad hoc sensor network. In: IEEE Wireless Communication and networking Conference (WCNC) (March 2002)
5. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In: Proc. 33rd Hawaii Int'l. Conf. Sys. Sci. (January 2000)
6. Lindsey, S., Raghavendra, C.: PEGASIS: Power-Efficient Gathering in Sensor Information Systems. In: IEEE Aerospace Conf. Proc., vol. 3, 9-16, 1125–1130 (2002)
7. Savvides, A., Han, C.-C., Srivastava, M.: Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors. In: Proc. 7th ACM MobiCom, pp. 166–79 (July 2001)
8. Li, C.F., Ye, M., Chen, G.H., Wu, J.: An Energy-Efficient Unequal Clustering Mechanism for Wireless Sensor Networks. In: IEEE International Conference on Mobile Adhoc and Sensor Systems MASS 2005, November 7-10, 8 p. (2005)
9. Tashtarian, F., Honary, M.T., Haghighat, A.T., Chitizadeh, J.: A new energy-efficient level-based clustering algorithm for wireless sensor networks. In: 6th International Conference on Information, Communications & Signal Processing 2007 (2007)

Measuring the Closed-Loop Throughput of 2x2 HSDPA over TX Power and TX Antenna Spacing

Sebastian Caban[1], José A. García-Naya[2], Christian Mehlführer[1],
Luis Castedo[2], and Markus Rupp[1]

[1] Institute of Communications and Radio-Frequency Engineering,
Vienna University of Technology, Vienna, Austria
[2] Department of Electronics and Systems,
University of A Coruña, A Coruña, Spain
`jagarcia@udc.es`

Abstract. Mobile network operators demand small base station antennas and high physical layer throughputs. In the downlink, high physical layer throughputs can be achieved by exploiting transmit diversity. Given that the correlation between different propagation paths reduces the achievable throughput, it is commonly conjectured that the greater the transmit antenna spacing, the better the radio link performance. The open question is, how much does the throughput of a communication system actually change over antenna spacing?

We answer this question by closed-loop throughput measurements at 2.5 GHz for standard compliant 2×2 HSDPA in a realistic, urban, outdoor scenario. The results are presented in terms of physical layer throughput over TX antenna spacing and TX power. We arrive at the somehow surprising conclusion that, for typical TX power values and typical antenna spacings, the throughput remains approximately independent with respect to the antenna spacing.

Keywords: Antenna diversity, Antenna spacing, Measurement, MIMO systems, Radio communications, HSDPA.

1 Introduction

The High-Speed Downlink Packet Access (HSDPA) mode [1] was introduced in Release 5 of the Universal Mobile Telecommunications System (UMTS) to provide high data rates to mobile users. This is achieved by employing techniques like fast link adaptation, fast Hybrid Automatic Repeat reQuest (HARQ), and fast scheduling. Multiple Input Multiple Output (MIMO) HSDPA was standardized in Release 7 of UMTS and is capable of increasing the maximum downlink data rate by spatially multiplexing two independently coded and modulated data streams. Additionally, channel-adaptive spatial precoding is implemented at the base station. The standard defines a set of precoding vectors and one of them is chosen based on a precoding control indicator feedback obtained from the user

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 388–399, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

equipment. Two different MIMO HSDPA modes are defined: the Transmit Antenna Array (TxAA) that utilizes two antennas to transmit a single stream, and the Double Transmit Antenna Array (D-TxAA) in which one or two streams (whichever leads to a higher throughput) are transmitted using two antennas. For comparison purposes, we defined additionally a two stream mode in which always two streams are transmitted.

A few experimental evaluations of HSDPA have been reported in the literature. For example, in [2] the throughput performance of a SISO HSDPA system is simulated based on so-called drive test measurements. Throughput measurement results of a SISO HSDPA system are presented in [3]. Finally, a non standard compliant MIMO HSDPA system was measured in [4]. However, apart from results published by the authors [5–7], we are not aware of publications showing the actual closed-loop throughput of a standard compliant MIMO HSDPA link.

The effects of antenna spacing at the transmitter and the receiver sides have been studied for a long time. First measurement campaigns carried out in outdoor scenarios date from the seventies (e.g. [8]). In these measurements, the **correlation coefficient** of the incoming signals with respect to antenna spacing was investigated. More recent measurements investigated this effect in indoor-only scenarios (e.g. [9]), in outdoor-to-indoor scenarios (e.g. [10]), and in outdoor-only scenarios (e.g. [11]).

The impact of antenna spacing on **channel capacity** has been measured intensively in a variety of scenarios and conditions, including indoor scenarios [12, 13], outdoor scenarios [12, 14, 15], reverberation chambers [16], and using virtual antenna arrays [17]. These measurement results were complemented with theoretical analyses (see [18–21] and references therein).

The **bit error ratio (BER)** has also been used as a metric for the evaluation of the performance of wireless systems with respect to the antenna spacing. In the literature, theoretic studies have been reported [22, 23]. Additionally, the influence of the antenna spacing on the BER has been evaluated in indoor [24, 25] and outdoor [26, 27] scenarios.

Recently, the influence of antenna spacing on the **throughput** of an OFDM transmission was studied in [28] by using sounded channel coefficients in a simulation. Similarly, [29] investigates the throughput difference between equally and cross polarized TX antennas. Remarkably, apart from [26, 28], all above cited references do not employ base station antennas similar to those currently in use in mobile cellular networks. Furthermore, except [28], none of the references found relates TX antenna spacing to the physical layer throughput of a standard compliant MIMO mobile communication system such as 2×2 MIMO HSDPA in our case.

2 Experimental Set-Up

The goal of the experimental set-up described below is to examine the impact of base station antenna spacing and polarization on the physical layer throughput

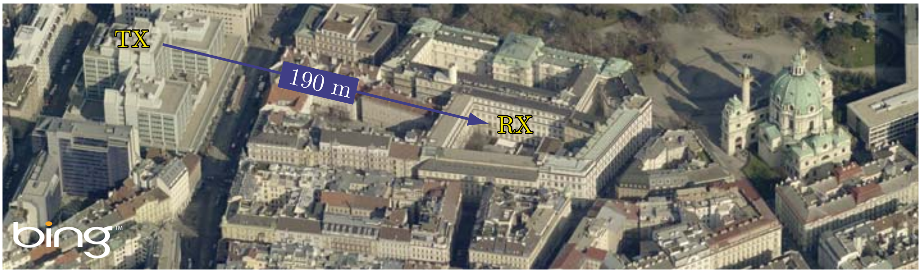


Fig. 1. Scenario overview [30]

of a standard compliant 2×2 MIMO HSDPA downlink transmission [1] under the following premises:

An Urban Outdoor Environment. We consider a realistic, non-line-of-sight scenario in the inner city of Vienna, Austria (see Figure 1). The TX antennas are placed on the roof of a tall building right adjacent to existing base station antennas of mobile phone operators (see Figure 2), making the measurement results obtained very realistic and representative for a mobile communication system. The RX antennas are placed in a small office (see Figure 3) at a distance of approximately 190 m (see Figure 1). The estimated root mean square delay spread for this rich scattering non-line-of-sight scenario is 0.5 µs (=1.9 HSDPA chip durations).

Closed-Loop Testbed Measurements. We employ closed-loop quasi-realtime testbed measurements as the hardware and experience required is readily available [5–7, 24, 31–33]. In our measurement approach, all possible transmitted data is generated off-line in MATLAB, but only the required data is then transmitted over a wireless channel which is altered by moving the receive antennas. The feedback calculation —mandatory for closed-loop HSDPA— is instantly calculated in MATLAB in approximately 40 ms (less than the channel coherence time). The received data itself is not evaluated in real-time but off-line using a cluster of PCs. Results for the scenario measured are automatically obtained using the same program that has already controlled the complete measurement procedure and documentation.

Flat Panel Antennas at the Base Station. At the base station, we employ two KATHREIN 800 10629 [34] 2X-pol panel antennas with a half-power beam width of 80°/7.5° and a total down tilt of 16° (= 10° mechanical + 6° electrical, see Figure 2). Each 2X-pol antenna consists of two cross-polarized antennas spaced by 0.6 λ (λ=12 cm at 2.5 GHz). Only two of the eight possible antenna elements are excited at the same time to obtain a two-element base station antenna with a variable element spacing from 0.6 λ to 7.7 λ for equal polarization, and 0 λ for cross polarization. Using two ordinary X-pol antennas instead of two 2X-pol antennas would have only allowed us to measure down to an element spacing of 1.3 λ, rather than 0.6 λ.

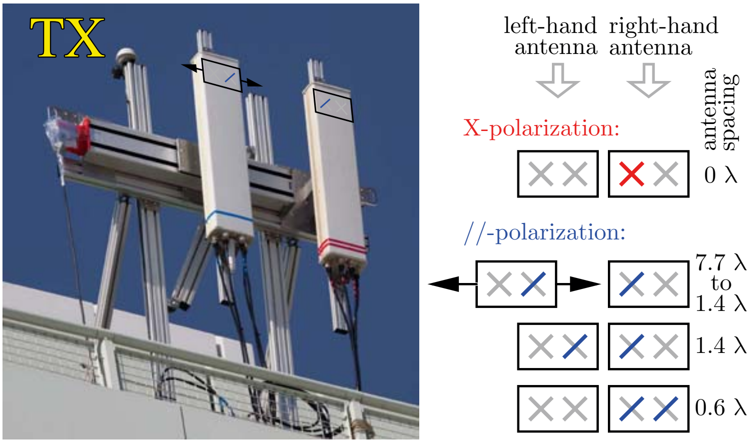


Fig. 2. A base station antenna consisting of a moveable 2X-pol antenna (left-hand) and a fixed 2X-pol antenna (right-hand). In total, only two antenna elements are excited at the same time.

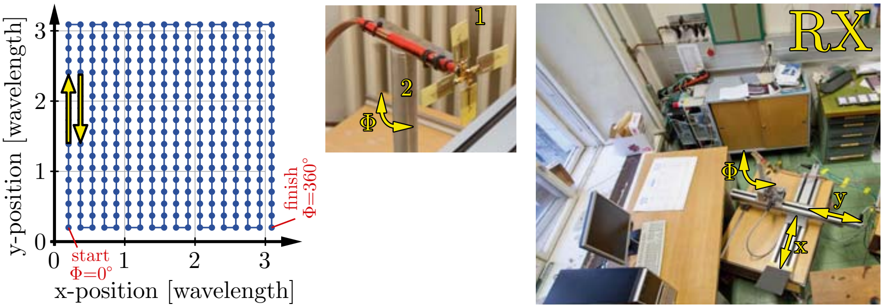


Fig. 3. The receiver employing two (1,2) moveable (x,y) and rotatable (Φ) printed monopole antennas. The other two printed monopole antennas shown are not used.

Two Printed Monopole Antennas at the Mobile Phone. At the receiver site, we utilize two realistic printed monopole antennas [35] that can be integrated into a mobile handset or a laptop computer. We employ differently polarized antennas to obtain robust and close to reality measurement results. As shown in Figure 3, we measure different receive antenna positions (x,y) in an area of $3\,\lambda \times 3\,\lambda$ to average over small scale fading and to avoid large scale fading effects. Because the antennas point into different directions, they experience a different average path loss. To average out this effect, we rotate the antennas (Φ) during the measurement.

A Standard-Compliant 2×2 MIMO HSDPA Transmission. We transmit standard compliant HSDPA data frames [1], including the pilot structure

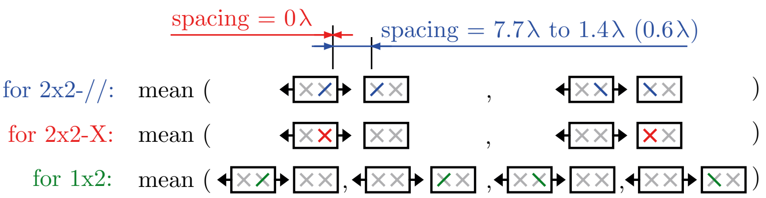


Fig. 4. Ensuring a fair comparison between 2×2 HSDPA with X-polarization, 2×2 HSDPA with //-polarization, and 1×2 HSDPA

[31, Chapter 3]. Three different HSDPA modes, either with equally (//) and cross-polarized (X) transmit antennas have been considered. In addition, a 1×2 SIMO mode has been also considered as a reference. In total, seven modes were measured:

- **One stream mode = TxAA** (1// and 1X). This is the so-called closed-loop Transmit Antenna Array (TxAA) mode with transmit diversity that uses strongly quantized precoding at the transmitter to increase the signal to interference and noise ratio (SINR) at the user equipment [31, pp. 48].
- **One-or-two stream mode = D-TxAA** (1or2// and 1or2X). This is the so-called Double TxAA mode (D-TxAA) that is downward compatible with TxAA. This mode equals TxAA when the SINR at the user equipment is low. At larger SINRs, D-TxAA switches to dual stream mode and transmits two independently coded HSDPA data streams. Thus, in TxAA, a single stream is always transmitted and in D-TxAA, either single-stream or double-stream is chosen [31, pp. 48] depending on which one leads to a higher physical layer throughput [36].
- **Two stream mode** (2// and 2X). For analysis purposes, we also implemented a two stream mode —non existent in the standard— that behaves like D-TxAA, but forces the transmitter to always use two streams, regardless of the SINR estimated at the receiver.
- **SIMO HSPDA** (1×2 SIMO). We measure 1×2 SIMO HSPDA as a reference and concomitant observations to enhance the precision of the 2×2 results measured over antenna spacing.

See [7] for a description of the procedure we use to measure in quasi real-time the closed-loop throughput of HSDPA by transmitting four frames: a "previous frame", a "data frame", and two possibly required retransmissions. More details about the algorithms used in the implementation can be found in [5]. Particularly, the channel estimation algorithm is described in detail in [37].

3 Inferring the Mean Scenario Throughput

When comparing the throughput of a "//-polarized transmission between 1.4λ and 7.7λ" to an "X-polarized transmission at 0λ" as shown in Figure 2, the main problem is that these transmissions use different antenna elements, thus experiencing a greatly different (up to 4 dB) average path loss. This problem can be overcome by averaging the throughput measured at different antenna elements as shown in Figure 4. In other words, to measure, for example, the throughput of the 2×2-TxAA-// mode, we average two measurements, one exciting both /-elements, the other one exciting both \-elements. A similar procedure is used to measure at 0.6 λ.

We use well known statistical techniques explained in e.g. [38–40] to infer the mean throughput performance of the urban scenario as described below (*the technical terms are given in italics in brackets*):

1) We measure the seven HSDPA modes to be compared (*grouping, comparison*) in random order (*randomization*) immediately after each other over the same channels (*blocking*) equally often (*balancing*).
2) We measure all above at 11 different transmit power levels (the abscissas in Figure 5.a, Figure 7.a, and Figure 8.a (*one-factor-at-a-time experiment*).
3) We measure all above at 12 different transmit antenna spacings (see Figure 2) when //-polarized TX antennas are used (see Figure 5.b, Figure 6, and Figure 8.b) (*11×12 full factorial design*). When X-polarization is employed, the antenna spacing is 0 λ, therefore the results are plot as dots on the ordinate (see Figure 7.b, and Figure 8.b).
4) We measure all above at 324 different receive antenna positions (see Figure 3) (*systematic sampling*).
5) We evaluate all measured throughputs off-line and average them (best estimator for the mean having no other knowledge, *plug-in principle*) over the RX antenna positions to obtain the mean scenario throughput (the ordinates in Figure 5, Figure 6, Figure 7, and Figure 8).
6) We use the correlation between the 2×2 throughput values and the 1×2 throughput values (*concomitant observations*) to enhance the precision of the 2×2 results measured over antenna spacing[1].
7) Finally, we calculate the 99% confidence intervals for the mean (the vertical lines in Figure 5, Figure 6, Figure 7, and Figure 8) to gauge the precision of the results shown (*BC_a bootstrap algorithm*).

4 Results Obtained

The results obtained are shown in the nine graphs plotted in Figure 5, Figure 6, Figure 7, and Figure 8.

Figure 5.a shows the mean scenario throughput over transmit power for the three HSDPA modes measured with //-polarized transmit antennas. We observe that transmitting one stream (1//) works as well as transmitting one or

---

[1] Looking at the 12 transmit antenna spacings measured, the 2×2 and 1×2 HSDPA throughputs are correlated (correlation coefficient 99%-confidence-interval=[0.87, 0.98], linear regression coefficient 99%-confidence-interval=[0.79, 1.24]) whilst the 1×2 throughputs should not change over antenna *spacing* but do change over antenna *position*.

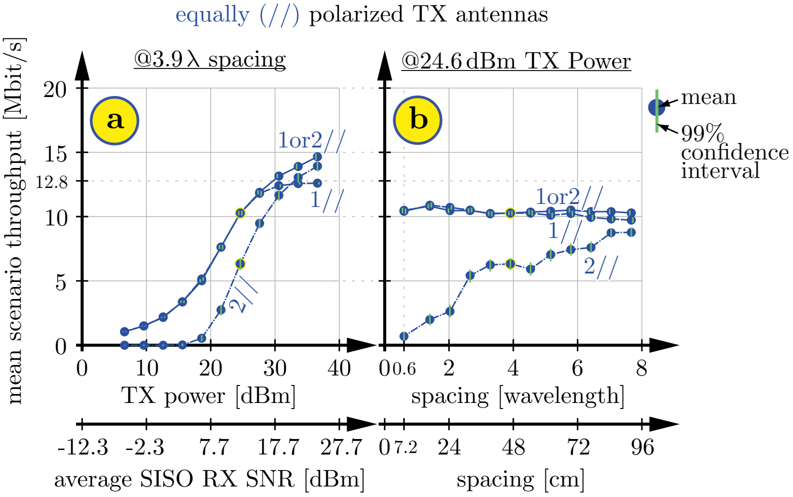


Fig. 5. Throughput of 2×2 HSDPA with 1 stream (=TxAA), 2 streams, and 1or2 streams (=D-TxAA) for equally (//) polarized transmit antennas

two streams (1or2//). Only at transmit power levels exceeding 27.6 dBm does transmitting one or two streams (1or2//) become advantageous because the 1// stream mode saturates at its theoretical maximum of 12.8 Mbit/s. Figure 5.a also shows how the transmission of two streams (2//) contributes to the high throughput achieved at high SINR values.

For antenna spacings greater than 5 λ, it can be seen in Figure 5.b that the 1or2// stream mode works slightly better than the 1// stream mode. This is because we have observed that the 2// stream mode works better than the 1// stream mode at some RX antenna positions.

Remarkably, the performance of the 2// stream mode is highly dependent on the TX antenna element spacing (see Figure 6.b). While the poor performance of the 2// stream mode at low antenna spacings is compensated by the excellent performance of the 1// stream mode (see Figure 6.a), the 2// stream mode outperforms the 1// stream mode at high transmit power values. The performance of the 1or2// stream mode is plotted in Figure 6.c, showing that the best performance is obtained when both 1// and 2// stream modes are combined.

Figure 7.a presents, over TX power, the three HSDPA modes measured with X-polarized elements at the transmitter. In contrast to //-polarization, the 1or2X mode is already better than the 1X mode at transmit power levels exceeding 13 dBm. As for X-polarization the active elements are always spaced by 0 λ, only dots on the ordinate are plot in Figure 7.b.

Because the results for equal and cross polarization are obtained by measuring at the same antenna elements (see Figure 4) we are able to directly compare the results shown in Figure 5 and Figure 7 in Figure 8.

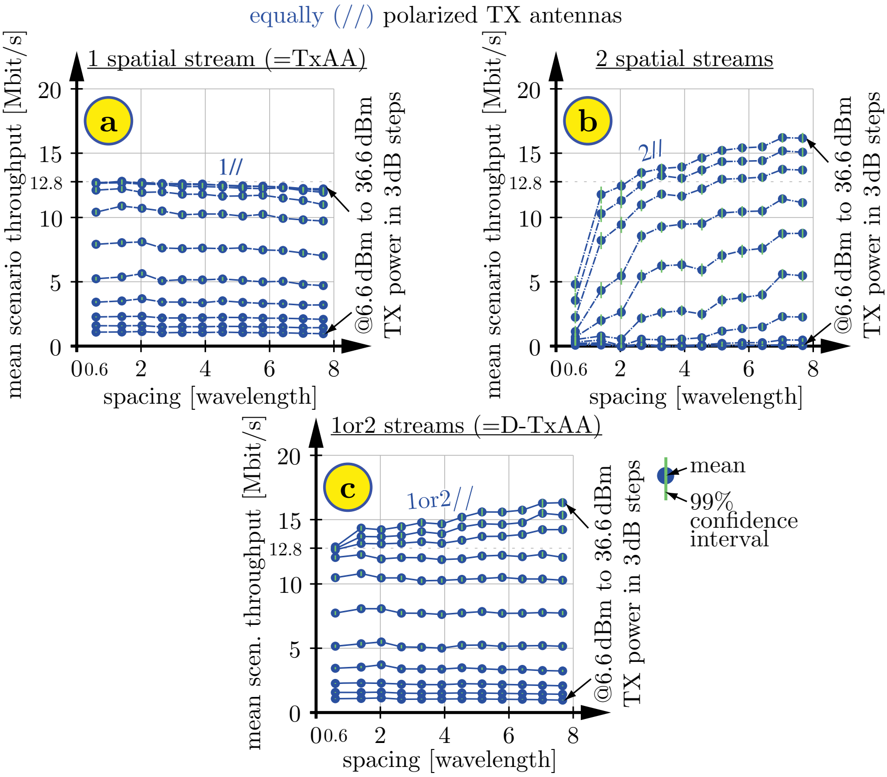


Fig. 6. Throughput of 2×2 HSDPA with 1 stream (=TxAA), 2 streams, and 1or2 streams (=D-TxAA) for equally (//) polarized transmit antennas

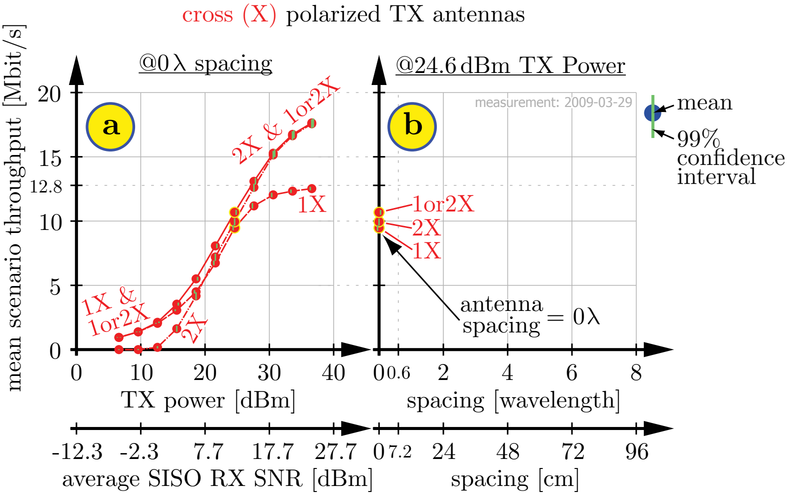


Fig. 7. Throughput of 2×2 HSDPA with 1 stream (=TxAA), 2 streams, and 1or2 streams (=D-TxAA) for cross (X) polarized transmit antennas

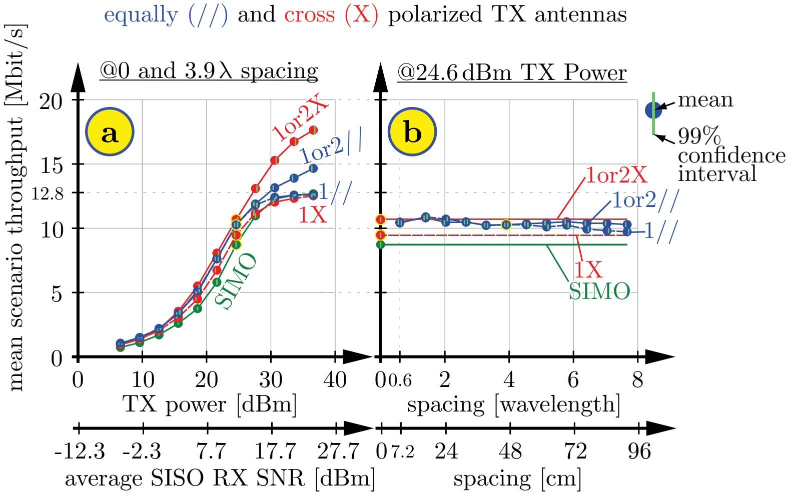


Fig. 8. Throughput of 2×2 HSDPA with 1 stream (=TxAA), 2 streams, and 1or2 streams (=D-TxAA) for equally (//) and cross (X) polarized transmit antennas

5 Conclusions

In this paper, the influence of TX antenna spacing and polarization on the closed-loop throughput of 2×2 MIMO HSDPA is investigated by testbed measurements. The measurement campaign was carried out in a realistic, urban, outdoor scenario in the inner city of Vienna with cross-polarized antennas at the receiver.

The results show that the 1or2X mode (D-TxAA with cross polarization) provides the highest physical layer throughput. On the contrary, polarization is not so important when only one spatial stream is allowed. Indeed, as shown in Figure 8, the performance of the 1// mode (TxAA with equal polarization) and the 1X mode (TxAA with cross polarization) is almost the same.

It is commonly conjectured that the throughput increases with the TX antenna spacing since separating the TX antennas provides higher spatial diversity due to lower correlation. However, the measurement results presented in this paper show that the throughput hardly depends on the antenna separation (see Figure 6.a, and Figure 6.c). Moreover, in some situations the throughput may even decrease with respect to antenna separation (see Figure 6.a). Only when the transmit power is relatively high (more than 27.6 dBm) and/or the 2// stream mode is used, the throughput clearly increases with respect to the antenna spacing (see Figure 6.b and Figure 6.c). However, for typical TX power values and typical antenna spacings, the throughput remains approximately independent of the antenna spacing.

Finally, it is very important to emphasize the influence of the antenna polarization on the physical layer throughput. The 2X and the 1or2X stream modes always outperform the 1or2// stream mode. Thus, more spatial diversity is obtained from using different polarizations rather than from using larger antenna spacings.

Acknowledgements. The authors thank Constantine Kakoyiannis for providing us with the printed monopole RX antennas. This work has been funded by the Christian Doppler Laboratory for Wireless Technologies for Sustainable Mobility. The authors thank Christoph Mecklenbräuker and their industrial partners, mobilkom austria AG and KATHREIN-Werke KG. This work has also been supported by the Xunta de Galicia, the Ministerio de Ciencia e Innovación of Spain, and the FEDER funds of the European Union under the grants 09TIC008105PR, TEC2007-68020-C04-01, and CSD2008-00010. The financial support by the Federal Ministry of Economy, Family and Youth and the National Foundation for Research, Technology and Development is gratefully acknowledged.

References

1. 3GPP. Tech. spec. group radio access network, physical layer procedures (FDD) (Tech. Spec. 25.214 V7.7.0) (2007)
2. Landre, J.B., Saadani, A.: HSDPA 14.4 Mbps mobiles - realistic throughputs evaluation. In: Proc. of VTC 2008, Spring, pp. 2086–2090 (2008), doi:10.1109/VETECS.2008.468
3. Holma, H., Reunanen, J.: 3GPP release 5 HSDPA measurements. In: Proc. PIMRC 2006 (2006), doi:10.1109/PIMRC.2006.254116
4. Riback, M., Grant, S., Jongren, G., Tynderfeldt, T., Cairns, D., Fulghum, T.: MIMO-HSPA testbed performance measurements. In: Proc. PIMRC 2007 (2007), doi:10.1109/PIMRC.2007.4394434
5. Mehlfühurer, C., Caban, S., Rupp, M.: MIMO HSDPA throughput measurement results in an urban scenario. In: Proc. 70th IEEE Vehicular Technology Conference (VTC 2009-Fall), Anchorage, AK, USA (2009), doi: 10.1109/VETECF.2009.5378994, `http://publik.tuwien. ac.at/files/PubDat_176321.pdf`
6. García-Naya, J.A., Mehlführer, C., Caban, S., Rupp, M., Castedo, L.: Throughput-based antenna selection measurements. In: Proc. 70th IEEE Vehicular Technology Conference (VTC2009-Fall), Anchorage, AK, USA (2009), doi:10.1109/VETECF.2009.5378992, `http://publik.tuwien.ac.at/files/PubDat_176573.pdf`
7. Caban, S., Mehlführer, C., Lechner, G., Rupp, M.: Testbedding MIMO HSDPA and WiMAX. In: Proc. 70th IEEE Vehicular Technology Conference (VTC2009-Fall), Anchorage, AK, USA (2009), doi:10.1109/VETECF.2009.5378995, `http://publik.tuwien.ac.at/files/PubDat_176574.pdf`
8. Lee, W.: Effects on correlation between two mobile radio base-station antennas. IEEE Transactions on Communications 21(11), 1214–1224 (1973)
9. Kivinen, J., Zhao, X., Vainikainen, P.: Empirical characterization of wideband indoor radio channel at 5.3 GHz. IEEE Transactions on Antennas and Propagation 49(8), 1192–1203 (2001), doi:10.1109/8.943314

10. Medbo, J., Harrysson, F., Asplund, H., Berger, J.E.: Measurements and analysis of a MIMO macrocell outdoor-indoor scenario at 1947 MHz. In: Proc. of VTC 2004 Spring, vol. 1, pp. 261–265 (2004)
11. Zhao, X., Kivinen, J., Vainikainen, P., Skog, K.: Propagation characteristics for wideband outdoor mobile communications at 5.3 GHz. IEEE Journal on Selected Areas in Communications 20(3), 507–514 (2002), doi:10.1109/49.995509
12. Jungnickel, V., Pohl, V., von Helmolt, C.: Capacity of MIMO systems with closely spaced antennas. IEEE Communications Letters 7(8), 361–363 (2003), doi:10.1109/LCOMM.2003.815644
13. Intarapanich, A., Kae, P., Davies, R., Sesay, A., McRory, J.: Spatial correlation measurements for broadband MIMO wireless channels. In: Proc. of VTC 2004 Fall, vol. 1, pp. 52–56 (2004), doi:10.1109/VETECF.2004.1399919
14. Skentos, N., Kanatas, A., Pantos, G., Constantinou, P.: Capacity results from short range fixed MIMO measurements at 5.2 GHz in urban propagation environment. In: Proc. of ICC 2004, vol. 5, pp. 3020–3024 (2004), doi:10.1109/ICC.2004.1313086
15. Chizhik, D., Ling, J., Wolniansky, P., Valenzuela, R., Costa, N., Huber, K.: Multiple-input-multiple-output measurements and modeling in Manhattan. IEEE Journal on Selected Areas in Communication 21(3), 321–331 (2003), doi:10.1109/JSAC.2003.809457
16. Kildal, P.S., Rosengren, K.: Correlation and capacity of MIMO systems and mutual coupling, radiation efficiency, and diversity gain of their antennas: simulations and measurements in a reverberation chamber. IEEE Communications Magazine 42(12), 104–112 (2004), doi:10.1109/MCOM.2004.1367562
17. Medbo, J., Riback, M., Berg, J.E.: Validation of 3GPP spatial channel model including WINNER wideband extension using measurements. In: Proc. of VTC 2006 Fall, pp. 1–5 (2006), doi:10.1109/VTCF.2006.36
18. Chizhik, D., Rashid-Farrokhi, F., Ling, J., Lozano, A.: Effect of antenna separation on the capacity of BLAST in correlated channels. IEEE Communications Letters 4(11), 337–339 (2000), doi:10.1109/4234.892194
19. Shiu, D.S., Foschini, G., Gans, M., Kahn, J.: Fading correlation and its effect on the capacity of multielement antenna systems. IEEE Transactions on Communications 48(3), 502–513 (2000), doi:10.1109/26.837052
20. Thushara, D., Rodney, A., Jaunty, T.: On capacity of multi-antenna wireless channels: Effects of antenna separation and spatial correlation. In: 3rd Australian Communications Theory Workshop (AusCTW) (2002)
21. Waldschmidt, C., Kuhnert, C., Schulteis, S., Wiesbeck, W.: Analysis of compact arrays for MIMO based on a complete RF system model. In: IEEE Topical Conference on Wireless Communication Technology, pp. 286–287 (2003), doi:10.1109/WCT.2003.1321527
22. Luo, J., Zeidler, J., McLaughlin, S.: Performance analysis of compact antenna arrays with MRC in correlated nakagami fading channels. IEEE Transactions on Vehicular Technology 50(1), 267–277 (2001), doi:10.1109/25.917940
23. Femenias, G.: BER performance of linear STBC from orthogonal designs over MIMO correlated nakagami-m fading channels. IEEE Transactions on Vehicular Technology 53(2), 307–317 (2004), doi:10.1109/TVT.2004.823475
24. Caban, S., Mehlführer, C., Mayer, L.W., Rupp, M.: 2x2 MIMO at variable antenna distances. In: Proc. of VTC 2008 Spring, Singapore (2008), doi:10.1109/VETECS.2008.276
25. Caban, S., Rupp, M.: Impact of transmit antenna spacing on 2x1 Alamouti radio transmission. Electronics Letters 43(4), 198–199 (2007), doi:10.1049/el:20073153

26. Hunukumbure, R., Beach, M.: Outdoor MIMO measurements for UTRA applications. In: Proc. of EURO-COST 2002 (2002), `http://hdl.handle.net/1983/887`
27. Trautwein, U., Schneider, C., Thomä, R.: Measurement-based performance evaluation of advanced MIMO transceiver designs. EURASIP Journal on Applied Signal Processing 2005(11), 1712–1724 (2005), doi:10.1155/ASP.2005.1712
28. Thomas, T.A., Desai, V., Kepler, J.F.: Experimental MIMO comparisons of a 4-element uniform linear array to an array of two cross polarized antennas at 3.5 GHz. In: Proc. of VTC 2009 Fall (2009)
29. Jungnickel, V., Jaeckel, S., Thiele, L., Krueger, U., Brylka, A., von Helmolt, C.: Capacity measurements in a multicell MIMO system. In: IEEE Global Telecommunications Conference, pp. 1–6 (2006), doi:10.1109/GLOCOM. 2006.645
30. (C) (2009), Microsoft Corporation (2009), `http://www.bing.de`
31. Mehlführer, C.: Measurement-based performance evaluation of WiMAX and HSDPA. Ph.D. thesis; Vienna University of Technology (2009), `http://www.nt.tuwien.ac.at/fileadmin/data/testbed/diss-mc.pdf`
32. Caban, S., Mehlführer, C., Langwieser, R., Scholtz, A.L., Rupp, M.: Vienna MIMO Testbed. EURASIP Journal on Applied Signal Processing, Article ID 54868 (2006), doi:10.1155/ASP/2006/54868
33. Mehlführer, C., Caban, S., Rupp, M.: Experimental evaluation of adaptive modulation and coding in MIMO WiMAX with limited feedback. EURASIP Journal on Advances in Signal Processing, Article ID 837102 (2008), `http://publik.tuwien.ac.at/files/pub-et_13762.pdf`, doi:10.1155/2008/837102
34. KATHREIN-Werke KG Antenna No. 800 10629 (2010), `http://www.nt.tuwien.ac.at/fileadmin/data/testbed/kat-ant.pdf`
35. Kakoyiannis, C., Troubouki, S., Constantinou, P.: Design and implementation of printed multi-element antennas on wireless sensor nodes. In: Proc. of ISWPC 2008, pp. 224–228 (2008), doi:10.1109/ISWPC.2008.4556202.36
36. Mehlführer, C., Caban, S., Wrulich, M., Rupp, M.: Joint throughput optimized CQI and precoding weight calculation for MIMO HSDPA. In: Conference Record of the Fourtysecond Asilomar Conference on Signals, Systems and Computers. Pacific Grove, CA, USA (2008), `http://publik.tuwien.ac.at/files/PubDat_167015.pdf`
37. Mehlführer, C., Rupp, M.: Novel tap-wise LMMSE channel estimation for MIMO W-CDMA. In: Proc. 51st IEEE Global Telecommunications Conference 2008 (GLOBECOM 2008), New Orleans, LA, USA (2008), `http://publik.tuwien.ac.at/files/PubDat_169129.pdf`, doi:10.1109/GLOCOM.2008.ECP.829
38. Fisher, R.: The Design of Experiments. Wiley, New York (1935)
39. Cox, D.: Planning of Experiments. John Wiley & Sons, Chichester (1958)
40. Efron, B., Hinkley, D.V.: An Introduction to The Bootstrap, 1st edn. CRC Monographs on Statistics & Applied Probability, vol. 57. Chapman & Hall, Boca Raton (1994), ISBN 0412042312

Towards Benchmarking of P2P Technologies from a SCADA Systems Protection Perspective

Abdelmajid Khelil, Sebastian Jeckel, Daniel Germanus, and Neeraj Suri*

Technische Universität Darmstadt,
Hochschulstr. 10, 64289 Darmstadt, Germany
Tel.: +49 6151 16{3414—3711—5321—3513}; Fax.: +49 6151 16 4310
`{khelil,jeckel,germanus,suri}@cs.tu-darmstadt.de`

Abstract. Supervisory Control and Data Acquisition (SCADA) systems are used to control and monitor critical processes. Modern SCADA systems are increasingly built with off-the-shelf components simplifying their integration into existing networks. The benefits of increased flexibility and reduced costs are accompanied by newly introduced challenges regarding SCADA security/dependability. Peer-to-Peer (P2P) technologies allow for the construction of self-organizing, dependable and large-scale overlays on top of existing physical networks.

In this paper, we build the base for using P2P to enhance the resilience of deployed SCADA systems. To this end, we provide a general analysis of both domains and their compatibility. In addition, we refine the existing classifications of P2P technologies w.r.t. the needs and capabilities of SCADA systems. Consequently, we identify core P2P-based protection mechanisms for SCADA systems, based on data and path replication. Our main results are generic guidelines for the exploitation of P2P technologies to enhance the SCADA resilience.

Keywords: SCADA, Critical Infrastructure Protection, P2P, Dependability, Security.

1 Introduction

For life in modern-day societies the dependability of Critical Infrastructures (CI), e.g., power grid or water supply, is of essential character. Supervisory Control and Data Acquisition (SCADA) systems are embedded in these CI for the purpose of monitoring and controlling them. While the first SCADA systems were built using proprietary standards and dedicated hardware in closed architectures, the trend is towards more flexible systems and open protocols like the Internet Protocol (IP). IP-enabled SCADA components allow usage of commercial off-the-shelf (COTS) products and integration into existing network structures, e.g., corporate LAN or WAN like the Internet, thus saving costs of specialized hard-/software and allowing faster adaption to changing requirements. At the same time, this technological shift towards a networked system, eventually

---

* Research supported in part by EU INSPIRE, CASED (www.cased.de), and EU CoMiFin.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 400–414, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

even connected to the Internet, introduces new threats and vulnerabilities to SCADA systems and since the disputed concept security through obscurity is no longer applicable, previously unnoticed or ignored security issues might now be exposed. To handle these security challenges, techniques from conventional networked systems can be transferred to the SCADA domain.

Unlike the classical client/server concept, where roles are strictly separated, in Peer-to-Peer (P2P) networks every node/peer is a client as well as a server. While at first mainly used for file-sharing, the active research attention P2P received led to several new application areas. There is a clear trend away from client/server towards P2P-based decentralized, self-organizing and fault-tolerant architecture. Similarly, the migration from the deterministic and client/server-like SCADA architectures towards P2P-like architectures is desired [1,2,3] in order to increase the SCADA resilience. However, such paradigm switch is challenging for operational, heterogeneous and difficult-to-replace SCADA systems. P2P overlays, through their inherent data and path replication mechanisms, allow to break the determinism of already deployed SCADA systems and consequently provide for a promising SCADA protection approach. The main contributions of this paper consist in providing generic guidelines for using P2P technologies to protect operational SCADA systems. In particular, we show how an appropriate P2P technique can be selected for a given SCADA system. This mapping is based on the SCADA system's properties, requirements and the specific application.

The rest of the paper is organized as follows. Section 2 gives an overview of SCADA systems, highlighting their characteristics and special needs. In Section 3, we briefly describe the most prominent P2P techniques and their underlying concepts and design motivations. Consequently, we provide a novel fine-tuned classification of P2P techniques according to SCADA-relevant properties. Section 4 details the requirements, prerequisites and architecture for P2P-enabling while discussing the potential usage scenarios of P2P to enhance the resilience of SCADA systems. In Section 5, we describe how one should proceed to select an appropriate P2P technique for a specific SCADA system. Section 6 presents conclusions and directions of future work.

2 SCADA Systems Overview

The purpose of SCADA systems is to allow remote human supervision of critical processes found in infrastructures, industrial sites or other facilities. The two main tasks of SCADA systems are (a) to collect process data and present it to an operator, and (b) to forward operator commands to the process where they get executed. In the following we will give an overview of how SCADA systems are built and how they operate.

SCADA systems are organized hierarchically. At the lowest level, sensors and actuators are embedded directly within the industrial processes. At the next level, Remote Terminal Units (RTU) are connected to possibly multiple sensors or actuators. A wide range of components can be used as RTU, such as ordinary personal computers, Programmable Logic Controller (PLC), and small-sized/custom devices. RTUs send their collected data via LAN or WAN to a

Master Terminal Unit (MTU). An MTU gathers accumulated sensor data from RTU, monitors the system and sends commands to actuators to adjust the system behavior. MTUs vary in size and can house (1) Human Machine Interface (HMI) stations, which visualize the system state for human operators, (2) database servers to store received information for record-keeping and analysis, (3) data acquisition nodes, which receive incoming data and forward it for further processing, and (4) data processing nodes to compute calculations on the received data and execute automated control loops. It is also possible for an MTU to consist of a single computer with only HMI software and a human operator. For large scale SCADA systems spanning over a wide geographical area, the hierarchy is extended with additional layers of supervisory stations.

The emerging networked topologies are highly flexible but also highly heterogeneous. Networked SCADA systems may be interconnected across whole nations and beyond, just as the corresponding infrastructures like power grids are. [4] gives an example for such a large scale system to monitor a power grid in the US, consisting of 270 utility stations at different locations with up to 50000 sensors at each of them. Fig. 1 shows an example topology for a networked SCADA system.

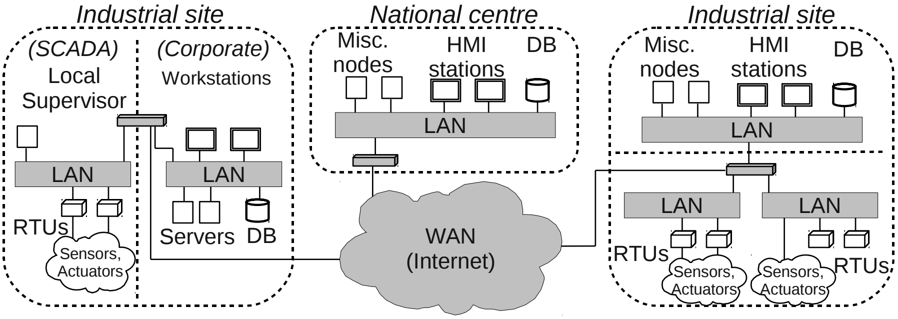


Fig. 1. Networked SCADA system

Data Flows and Timeliness Requirements: Three types of control loops can be identified. (i) Safety-critical control loops are realized at RTU level and normally implement emergency protocols to shut down or throttle the process if communication with the supervisor is interrupted or a critical incident is imminent. The timeliness constraints for such control loops are in the millisecond-to-second range to allow very fast responses to potential safety threats. (ii) Operation-critical control loops are necessary for the process to perform its tasks properly. They may involve several entities at supervisory level, including human operators. Since one RTU usually is just one among many, these control loops handle coordination backed by system-level intelligence and aggregated information to realize complex tasks that involve multiple entities. The timeliness requirements are less strict here and delay up to several seconds or even minutes might be acceptable depending on the concrete scenario. However, to enable remote supervision of a process in real-time, low latency for these control loops is desirable.

(iii) Non-critical control loops are used for process optimization, record-keeping, higher-level coordination, etc. Their failures can be compensated and do not critically affect the system. Summarizing, there are two main, unidirectional data flows in a SCADA hierarchy: (1) Sensor data, upwards from sensors to higher levels, and (2) control commands, downwards from higher levels to actuators. In addition, multiple supervisory stations may exchange their data.

The Main SCADA Perturbations: Based on [5] the perturbations identified for digital, packet-based messaging of SCADA are delay, jitter, transient loss, permanent loss, eavesdropping and injection. Delayed messages are prevented from arriving at their destination in time. For messages from sensors this could mean that the operator is informed of dangerous situations too late. Jitter is a form of delay, where messages arrive out of order so they fail their intended purpose. Similarly, transient or permanent message loss may disturb the proper operation of the SCADA system. Unlike these accidental perturbations, eavesdropping and message injection are deliberately conducted by an attacker. Usually, eavesdropping serves the purpose of collecting data about the system used to prepare further attacks. With message injection an attacker can send his own commands to actuators or report fake sensor data to operators, either to hide the real process state or to maneuver them into taking inappropriate actions.

3 SCADA-Driven Classification of P2P Technologies

After briefly surveying the existing P2P technologies, we present a new classification for the selection of an appropriate P2P technology to protect SCADA systems in the presence of faults.

3.1 Overview of P2P

Generally, an overlay network - or short just overlay - is a virtual network constructed on top of another physical one, which is called underlay accordingly. Comprehensive surveys of existing P2P technologies can be found in [6] and [7].

First-generation Systems - Unstructured Overlays: The first applications that popularized the term P2P and its underlying technologies were mainly used to share digital music or other small media files for a large number of Internet users. The traditional client/server architecture shows both a poor scalability and fault-tolerance since it centralizes the storage, indexing, search and transfer of data. Instead of storing all the data, the first P2P technique Napster uses a server only to maintain an index of all shared objects and the corresponding users and to provide for an efficient search. The file storage and transfers only involve the users. Gnutella [8] provides a fully decentralized P2P architecture. This is achieved by decentralizing the storage, indexing, search and transfer of data, which is now completed by users/peers without relying on any centralized entity. Gnutella mainly uses flooding for topology and data management. When new peers join a Gnutella overlay they are more likely to connect to an already well connected node (the integration of new peers follows a power law). Consequently, the performance and fault-tolerance of the overlay depends on these well-connected node. Performance studies pointed out Gnutella's poor performance. Gia [9] improved Gnutella performance through a designing a flow control mechanism, using random walk instead of flooding and adapting the topology to the capacity of peers. FastTrack [10] improved Gnutella's design and made it scalable with acceptable performance. It did so by exploiting the invariants that peers are highly heterogeneous w.r.t. to their capabilities and that the probability for a peer to leave the network is inversely proportional to its current up-time. Where Gnutella treated all peers equal, FastTrack promotes ordinary peers that are able and willing to take over more responsibilities to so called super peers.

Second-generation Systems - Structured Overlays: The decentralized P2P systems introduced so far have problems to locate data efficiently and correctly at the same time, especially for systems with many peers. Compared to centralized systems, they lack a global index that contains the location of all data objects existing within the network. Trying to maintain such a complete index for every peer individually does not scale because each one would need to keep track of every object in the network, resulting in huge coordination complexity. The P2P systems described next use the concept of a Distributed Hash Table (DHT) to replace the keyword-based searching found in first-generation systems. For a DHT, the hash buckets are distributed among the peers in an overlay network. So to look up the value associated with a given key, the peer responsible for the respective bucket has to be found first. Therefore, the supported operations of a DHT are reduced to lookup(k) with changed semantics so that it returns the peer responsible for the given key k. To retrieve, store or delete a value this peer has then to be contacted directly. The terms routing time and look-up time can be used interchangeably, as the look-up of a key simply means routing towards it. The challenge of implementing a DHT is to realize overlay routing for a fully decentralized topology, so that starting from an arbitrary peer, the one responsible for any given key can be found in a fast and efficient way.

There are many different DHT implementations and the most prominent representatives are Chord [11], CAN [12], Tapestry [13], Kademlia [14], Pastry [15], Koorde [16] and Kelips [17].

P2P Applications: Generally, an overlay can extend the underlay's features or modify its behavior, for example by adding an additional layer of security like VPN do, without breaking compatibility or making changes to existing protocols. This makes overlays especially attractive for use over networks like the Internet, where modification of currently used protocols is not an easy option. P2P systems use application-layer overlay networks to realize decentralized organization such as efficient multicast/streaming [18], distributed storage [19] or event notification [20]. While the last two could also be put to use in SCADA systems, the primary interests are overlay features and applications that increase resilience. [21] uses a structured overlay to overcome link failures by replicating data at other peers. In [3] a concrete implementation of overlay networks for power grids is presented. These approaches are considered as a starting point to explore additional P2P applications or techniques that could be used in a general SCADA system context.

3.2 P2P Classification

Because the conventional classification of decentralized system (structured vs. unstructured) only relates to their basic underlying principles and does not cover any specific details, in this section fully distributed P2P technologies will be classified w.r.t. to the aspects relevant for SCADA protection.

Benchmarking Criteria: The first step necessary to effectively compare and benchmark P2P systems is an analysis of their distinctive properties and features. To capture the relevant properties of P2P systems, the following indicators are commonly used: Topology of the overlay, average length of paths, routing overhead, maintenance overhead, average peer degree, overlay dynamics, overlay determinism, routing latency, state size on peers, self-optimization, locality, load balancing, heterogeneity of peer roles, overlay robustness and security level. Evaluation and benchmarking criteria should consider these indicators. With the SCADA applications in mind, the focus is on the following benchmarking criteria for given reasons: (1) Routing latency, due to stringent SCADA timeliness requirements, (2) minimum requirements, because of limited capabilities of legacy SCADA components, (3) communication overhead, since P2P traffic should not block SCADA communication, and (4) robustness and security, as these are the aspects that should be improved for SCADA systems.

Routing Latency: The overlay capabilities of structured and unstructured systems differ as the former can use directed routing while the latter have to search blindly, for example by flooding. This has a significant effect on the upper bound of routing steps. For structured systems with N peers, this is $O(\log N)$ or better, depending on the implementation. For unstructured systems it is $O(N)$. Albeit this worst case is highly unlikely, especially when using optimized architectures like [9], it generally shows that for large systems paths are not theoretically bounded in length and may become very long (Fig. 2 left). Short paths are crucial for low latency as each additional step not only brings obvious additional delay but also raises the chance to encounter a low quality link. However, there is no guarantee that these may not be found on short paths as well. That is why to truly minimize routing latency self-optimizing and/or locality-aware techniques have to be used. Finding short paths also depends on the node degree: The higher the number of neighbors, the higher is the chance to find one close to the destination.

Minimum Requirements: The amount of required memory mainly depends on the node degree. All introduced structured networks have fixed upper bounds that are supposed to be reached because of overlay-specific invariants required for efficient routing. This allows little flexibility for individual peers w.r.t. heterogeneous capabilities, so the weakest peers in the network actually dictate the maximum possible state size for all others (Fig. 2 right). Unstructured networks have better support for heterogeneity because in a random overlay it doesn't matter if some peers are only able to manage a few connections as long as the average node degree is high enough to keep the graph connected. For peers with very low capabilities, hybrid topologies can relief them of any P2P-specific requirements so they are just in a client/server relationship with another peer.

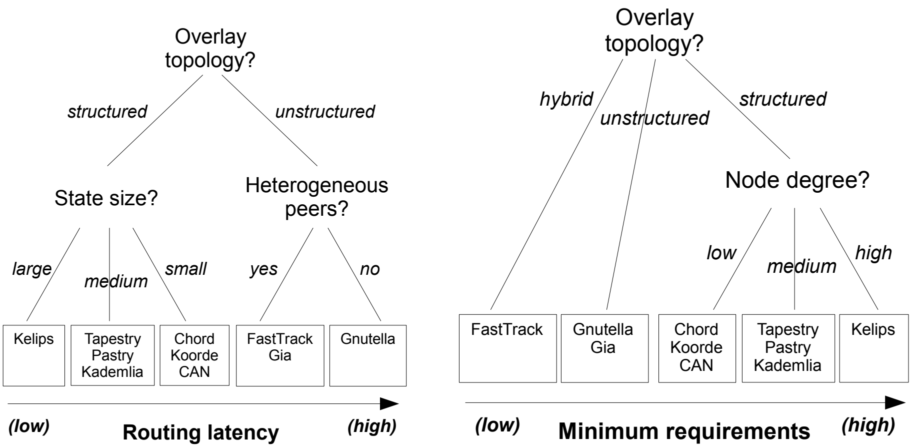


Fig. 2. Routing latency and minimum requirements

Communication Overhead: What is included here is the overhead for routing and maintenance (Fig. 3). The former varies with the supported overlay operations since flooded messages spread exponentially resulting in excessive amounts of unnecessary communication when only addressing a single target. Structured systems, on the other hand, usually don't cause additional routing traffic unless it is for redundant messages or concurrent routing to increase reliability or lookup speed. The influences on maintenance overhead are state size and specifically node degree. Connections to neighbors have to be kept up-to-date by checking for disconnected peers, updating meta-data like roundtrip time, etc. Rigid and complexly constructed overlay structures generally result in higher message overhead to integrate new peers or handle membership changes. This implies that unstructured systems have little maintenance overhead, or at least for them it can be reduced to a low level because there is no fear that the overlay structure might degrade. The deployment of P2P should not impact negatively the underlying SCADA application by excessively consuming network bandwidth. To overcome this issue, [22] proposes to model the overlay network and bandwidth availabilities as a minimization problem. The problem is NP-Hard and a heuristic for a distributed algorithm to continuously adapt P2P neighbour relationships was developed. The adaption results in topologies that do not excessively stress peers with low bandwidth capacities. This supports high message availability and low timeliness because messages do not get stuck due to congestion. The overlay adaption process is repeated regularly because bandwidth provision in large-scale networks is subject to variations.

Depending on the implementation, dynamic topologies, for example caused by self-optimization, either have a positive or a negative impact on maintenance. That is because when using routing messages to update the overlay at the same time, no explicit maintenance communication is necessary. On the other hand, if self-optimization causes additional messages this increases the overhead. The

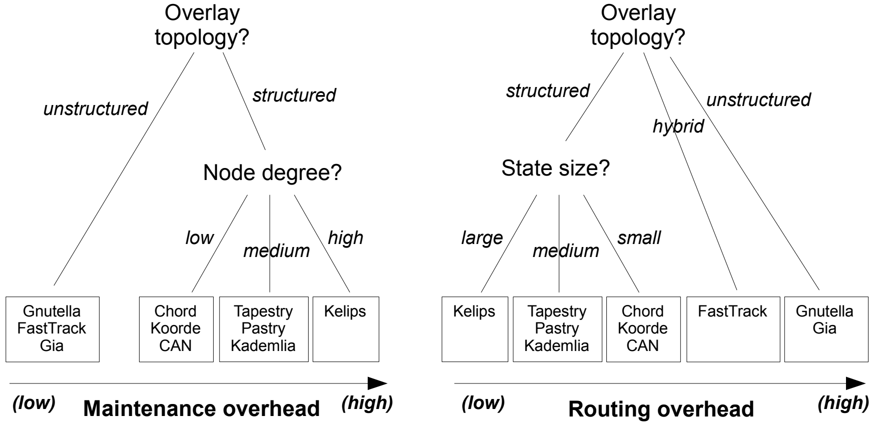


Fig. 3. Communication overhead

same statements in the last paragraph about state size and support for heterogeneity hold here as well.

Robustness and Security: Examining robustness against random failures for unstructured overlays, [23] shows that when comparing pure random graphs to those constructed by a power law, the latter are much more resilient when a very high number of peers (e.g., more than 20%) are dropped. The ability of structured systems to handle randomly failing peers depends on node degree as shown in [16]. With an average degree of $O(\log N)$, a structured system can theoretically recover even if 50% of the peers fail. The situation changes for targeted attacks. Generally, whenever responsibilities are concentrated at a few nodes, for example because of heterogeneous capabilities, these make preferred targets for an attack as their breakdown has great potential to disrupt the overlay. This also holds for power law networks when attacking the nodes with highest degree. Though only having an indirect impact, load balancing also helps to increase overlay robustness as it counteracts failure of nodes due to an overwhelming number of requests. Failures that are locally concentrated, for instance caused by the effects of a disaster, also lead to multiple overlay failures in close proximity to each other. It would be safer regarding overlay stability if these failures were evenly distributed across the overlay. The most important aspect about security is how easy it is for an attacker to make reasonable assumptions about the system. Rigid, deterministically constructed overlays as found in some structured systems allow an attacker who is able to deduce information from intercepted messages to build up knowledge about the system state; it may even be possible to predict behavior purely based on algorithmic details. Dynamic topologies make it hard to learn about the system and consequently complicate a successful attack. Due to the decentralized nature of P2P systems, attackers are required to control either a large fraction of peers in the network to gain control over it, or they are required to introduce peers at specific locations either in the address space or in the topology to enable their malicious intent. Two famous attacks in this context are the Sybil attack [24] and the Eclipse attack [25]. Both attacks require either introduction or hijacking of notable amounts of peers. The following two basic measures may avert these attacks. (1) The peer ID assignment needs to be safe, e.g., physical machines must not be admitted to join the overlay network with multiple IDs at the same time. (2) Topologies should not be open for extension, i.e., contrary to file sharing networks, some serious applications may define a fixed set of nodes that is allowed to participate in the overlay network and thereby excludes newly introduced nodes on behalf of an attacker. The second measure can be realized by using an admission protocol [26].

4 Increasing SCADA Protection with P2P Technology

Now that an overview of both SCADA and P2P technologies has been given, we will attempt to bring them together. This is achieved by discussing general feasibility, technical prerequisites and architecture, and analyzing prospective applications.

4.1 P2P-Enabling: Requirements, Prerequisites and Architecture

Because of the critical nature of security and dependability for SCADA systems, the following basic objectives should be followed when applying P2P techniques: (1) The underlying SCADA system's dependability and in particular QoS[1] should not be degraded and the overall system resilience should be increased, and (2) solutions to newly introduced P2P vulnerabilities must exist and their costs should not outweigh the P2P benefits. The P2P overlays introduced so far are built for use in a large-scale network, namely the Internet, so to qualify as a peer a computer must be connected and implement the Internet Protocol Suite to be able to communicate. The INSPIRE project [27] shows how P2P can be integrated into the SCADA message flow by adding an additional middleware layer, where all P2P-related functions are realized. This middleware should be supported by an underlying operating system for a peer to take a full part as a member of the overlay.

We follow an intrusive, active monitoring approach of SCADA systems, contrary to [1,2], which design a P2P-based passive monitoring architecture for smart micro power grids as a specific type of SCADA system. Working with a fixed and well-known population even allows for a minimal overlay maintenance overhead. As P2P architectures are usually open for new, unknown participants, these systems inherently do not offer any methods for access control. These have to be implemented since SCADA systems are necessarily closed and must only consist of well-known entities.

4.2 Potential P2P Benefits for SCADA

Considering a representative scenario in which an interruption of the SCADA message flow has been detected, e.g., from an RTU to a server in the MTU, we preset

---

[1] QoS refers to message delivery time, quantifiable by calculating values for mean, maximum and standard deviation.

different possible applications that can be implemented when using a P2P overlay to maintain the SCADA resilience. Naturally, as structured and unstructured architectures differ in functionality, so does the way these applications on top of them are implemented. The two basic methods to exchange data between the otherwise disconnected entities are rerouting and replication. Rerouting means that the RTU (re)sends its messages via overlay to the server, representing a push approach. For replication on the other hand the RTU's data is replicated at alternative locations where the server can pull it from. Though per definition replication has a slightly larger communication overhead since it is done in two steps, ultimately the SCADA application may dictate which method to use. Another distinction is made between direct and indirect rerouting: Either the overlay is used to directly transfer the message itself, or just to find and establish an intact path to the server that can subsequently be used. Which method is more efficient depends on multiple factors: For large message sizes it is better to find a short, high quality path first instead of transmitting large amounts of data over multiple hops with potential delay and/or low throughput; the same goes for frequent message loss, in which case one path can be reused multiple times. For small messages and/or transient loss direct sending is better suited since there is no overhead. For replication, the two basic approaches are to either wait until a failure has been detected and then react, or to proactively replicate all data regardless of failures. Unlike reactive replication, the latter strategy will cause permanent background traffic and require a constant amount of memory. It has the advantage that no coordination between the replicating RTU and the server is necessary and failure detection capabilities are only required on the server side. In the following, we discuss general implementation strategies for rerouting and replication in unstructured and then structured P2P overlays.

Applications for Unstructured P2P Systems. *Rerouting:* As explained earlier, unstructured systems do not support directed routing towards a certain destination; instead the overlay has to be searched randomly, e.g., by using a distributed algorithm based on random walk or flooding. What is different for routing compared to object search is that ultimately the destination of the message is already known. This means it is not necessary to route through the overlay exclusively until the server is reached; once an arbitrary peer that still has a functioning connection to the latter is found, delivery can proceed through the underlay from there on. This is desirable considering that every further hop once a working path is available only increases delay without any benefit. Based on this idea, for direct rerouting messages are simply forwarded through the overlay until a peer can deliver them. A flooding-based algorithm is likely to find such a peer faster as it can search along multiple paths at once at the price of higher bandwidth consumption and possibly redundant message delivery. Random walking will not cause additional traffic but is likely to take longer when forwarding over multiple hops. All this also applies to the indirect method, but with a modified procedure: First find a peer p that can reach server s, e.g., by using flooding or random walk. Then send messages via p to s. Since not the data messages themselves are used but only requests on who can reach s, the overhead is not as large as it would be for same technique with direct rerouting, thus making flooding more attractive for this approach.

Replication: In unstructured systems data replication is realized by distributing data to multiple peers. Due to the random nature of the overlay there is no way to deterministically find out where a certain data object will be replicated. The server has to search for the data. Unlike for rerouting, here it's not possible to take any shortcuts, because replication is realized on top of the overlay. Reactive replication will start forwarding its messages to its neighbors once a failure has been detected. Additionally, it will send a notification to the server via overlay, causing him to start searching. Since it takes some time until new data has spread across a system with many peers and reasonable bandwidth limits, the time until the failure is detected, plus the time until the server has received the notification, plus the time for the server to find it while still sparsely replicated is likely to exceed SCADA timeliness constraints. Proactive replication will require a constant amount of background traffic and memory. [28] shows optimal strategies on how to select peers for replication to minimize search time and maximize discovery rate. Nevertheless, replication in other than small-scale unstructured systems seems to be a poor choice when compared to rerouting as it takes longer, is more complicated and yet consumes more bandwidth and memory.

Applications for Structured P2P Systems. *Rerouting:* The general premises and features established for unstructured systems hold here. Since in structured networks peers are addressed by routing towards them, a proposed algorithm for direct rerouting is to forward a message along its overlay path to its destination and checking for an available underlay connection at every hop to directly deliver it, well aware that for exclusive overlay routing this would lead to congestion close to the destination. Indirect rerouting, with sender p, receiver s and message m could be implemented by first looking up peer q, who is responsible for m, and then sending m via q to s. While for pure overlay rerouting unstructured systems would clearly outperform structured ones, this is not the case here. Getting closer to the destination with every hop in the overlay does not relate to the probability of encountering a node with a non-broken underlay path to the former.

Replication: Replication in structured systems can be realized by using all peers in the overlay for distributed data storage, accessible over the DHT interface. As structured networks offer more functional possibilities, there are many possible algorithms. An example given in [21] for a reactive approach originated by the sender p of a data message m on failure detection works in three steps: First, m is stored in the DHT with its unique identifier. Then, the server s, which was the original recipient for m detects (through the SCADA application logic) the loss or delay of m. Finally, s can retrieve m from the DHT. Another schematic algorithm, this time for proactive replication: Every peer p deterministically picks i random surrogate peers $q_1, q_2, \ldots, q_i$, at which it replicates its data. As soon as a server can't reach p it instead tries to obtain the required data from the surrogates. In conclusion, structured systems are well suited for data replication since they have scalable upper bounds and offer built-in load balancing.

5 Mapping P2P Techniques to SCADA Systems

After discussing the general applicability of P2P technologies for SCADA protection, we now investigate how to select a specific P2P technique for a given SCADA system. Our P2P technology mapping onto SCADA systems is generic and considers the generic rerouting and data replication mechanisms and does not make any assumptions regarding scale, capabilities or topology of the SCADA system. Generally, it might not be appropriate to deploy a single P2P overlay on top of the whole SCADA system, e.g., to preserve locality of privacy of data. In such a case, different parts of the system have to be viewed and analyzed separately. Consequently, one should first identify the logical subsystems, and then select a suitable P2P technique for each subsystem.

5.1 Identification of Subsystems

There exist a number of mandatory criteria for partitioning the large-scale SCADA system: (a) Physical network topology as peers must be able to communicate etc, (b) security policies that may close off certain parts of a system to prevent external access or information leaks, and (c) ownership, as different parts of the system may be operated by different entities, thus should belong to different overlays. Additionally, included are legal obligations, regulations or political reasons. The resulting subsystems are unique, so a single one might be created for a number of reasons. Besides these non-negotiable aspects, further subsystems can be created based on the data flow model. It might be a bad idea to send operation-critical and non-critical message over the same overlay as both have very different requirements. The same goes for small-sized messages and larger ones. On the other hand, since many P2P properties like robustness increase with scale, overlays should be shared if possible. Fig. 4 shows an example of how multiple subsystems are identified within a generic SCADA hierarchy. The resulting subsystems are not necessarily disjoint, since points acting as bridges between two SCADA layers may be contained in two or more of those.

5.2 Selection of Appropriate P2P Techniques

Once a subsystem has been identified, a specific P2P technique can be selected, depending on the following aspects: (1) Scale, i.e., the number of peers meeting the P2P prerequisites, (2) requirements, i.e., certain properties the SCADA applications expect, e.g., timeliness constraints, communication model (push/pull), reliability etc, and (3) capabilities, i.e., peer resources and capabilities, i.e. memory, computational power, bandwidth, etc.

Assuming P2P is feasible, the first major choice is selecting the type of P2P application. Two possible options were discussed in Section 4.2, namely rerouting and data replication.

For rerouting, the use of a unstructured overlay is suggested, for the reasons given in Sections 3.2 and 4.2. In short these are:(1) High overlay flexibility w.r.t. to minimum requirements, node heterogeneity, selection of neighbors etc, (2) the overlay itself is very scalable, only searching in it is not. For rerouting this is not an

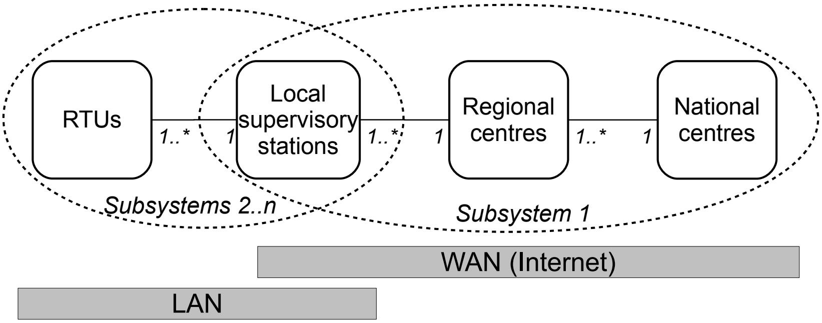


Fig. 4. Subsystem identification

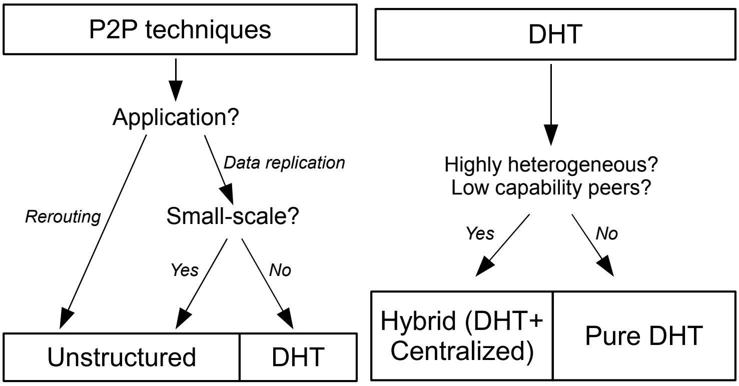


Fig. 5. Decision tree for basic technique

issue since the underlay is used as soon as possible, (3) a random topology which is hard to predict and robust against failures, and (4) Low maintenance overhead.

For data replication the case is more complex. Generally, DHT are preferred (see Section 4.2), however, for small-scale systems these make little sense since all properties regarding load balancing, neighbor selection etc. converge only for a high number of peers. Because of this, small-scale data replication is best realized with a highly connected unstructured overlay comparable to RON. Fig. 5 (left) summarizes the decision tree up to this point.

Because DHT don't support heterogeneous peers, the peers with the lowest capacities set the upper bound. So if there happens to be a big gap in terms of capabilities between the peers, a hybrid system should be considered, where the weaker peers are being managed by the stronger ones. This generally holds for situations where a minority thwarts overall performance.

In Section 3.2 three basic classes were identified, with respectively high, medium or low needs. To decide which concrete DHT to use one has to balance between requirements, capabilities and scale. Assuming that performance should be prioritized in terms of routing latency and robustness, this is achieved by utilizing as much capacities as possible. In Fig. 5 (right) the decision tree is completed for DHT.

6 Conclusions and Future Work

This paper provided a comprehensive analysis and classification of existing P2P technologies and their abilities to fulfil a SCADA system's needs. The pitfalls when using P2P techniques in a SCADA context were identified and a set of guidelines and best practices on how to avoid them were established. Previously designed P2P approaches were integrated into a taxonomy and their algorithmic principles were compared to those of other, newly proposed methods. To map specific P2P technologies to a given system, it was first shown how to partition it into different classes. The selection of appropriate techniques for each of those classes was based on previously drawn conclusions. This paper developed basic rules and concepts for the combination of SCADA and P2P. Furthermore, the analysis of P2P technologies for these specific types of applications provides a foundation for future research such as the application of the described methods for concrete SCADA systems to gain additional insights. Furthermore, trustworthiness measures should be developed to quantify and assess the overall increase of SCADA resilience through the P2P-enabling.

References

1. Beitollahi, H., Deconinck, G.: Analyzing the Chord Peer-to-Peer Network for Power Grid Applications. In: Fourth IEEE Young Researchers Symposium in Electrical Power Engineering (2008)
2. Beitollahi, H., Deconinck, G.: Peer-to-Peer Networks Applied to Power Grid. In: Proceedings of the International conference on Risks and Security of Internet and Systems, CRiSIS (2007)
3. Deconinck, G., Vanthournout, K., Beitollahi, H., Qui, Z., Duan, R., Nauwelaers, B., Lil, E., Driesen, J., Belmans, R.: A Robust Semantic Overlay Network for Microgrid Control Applications. In: Proceedings of the Workshop on Software Architectures for Dependable Systems, WADS (2008)
4. Fernandez, J.D., Fernandez, A.E.: SCADA Systems: Vulnerabilities and Remediation. Journal of Computing Sciences in Colleges 20(4) (2005)
5. Krutz, R.L.: Securing SCADA Systems (2005)
6. Lua, K., Crowcroft, J., Pias, M., Sharma, R., Lim, S.: A Survey and Comparison of Peer-to-Peer Overlay Network Schemes. IEEE Communications Surveys and Tutorials 7(2) (2005)
7. Androutsellis-Theotokis, S., Spinellis, D.: A Survey of Peer-to-Peer Content Distribution Technologies. ACM Computing Surveys, 36(4) (2004)
8. The Gnutella Protocol Specification v0.4 (2000), `http://www.stanford.edu/class/cs244b/gnutella_protocol_0.4.pdf`
9. Chawathe, Y., Ratnasamy, S., Breslau, L., Lanham, N., Shenker, S.: Making Gnutella-like P2P Systems Scalable. In: Proceedings of the 2003 ACM SIGCOMM Conference (2003)
10. Reverse Engineered FastTrack Protocol Specification, `http://cvs.berlios.de/cgi-bin/viewcvs.cgi/gift-fasttrack/giFT-FastTrack/PROTOCOL?revision=1.19`
11. Stoica, I., Morris, R., Karger, D., Kaashoek, F.M., Balakrishnan, H.: Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications. In: Proceedings of the 2001 ACM SIGCOMM Conference (2001)

12. Ratnasamy, S., Francis, P., Handley, M., Karp, R., Schenker, S.: A Scalable Content-Addressable Network. In: Proceedings of the 2001 ACM SIGCOMM Conference (2001)
13. Zhao, B.Y., Huang, L., Stribling, J., Rhea, S.C., Joseph, A.D., Kubiatowicz, J.D.: Tapestry: A Resilient Global-Scale Overlay for Service Deployment. IEEE Journal on Selected Areas in Communications, 22(1) (2004)
14. Maymounkov, P., Mazières, D.K.: A Peer-to-Peer Information System Based on the XOR Metric. In: Proceedings of the 2nd International Workshop on Peer-to-Peer Systems, IPTPS (2002)
15. Rowstron, A.I.T., Druschel, P.: Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems. In: Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms, Middleware (2001)
16. Kaashoek, F., Karger, D.R.: Koorde: A Simple Degree-Optimal Distributed Hash Table. In: Kaashoek, M.F., Stoica, I. (eds.) IPTPS 2003. LNCS, vol. 2735, Springer, Heidelberg (2003)
17. Gupta, I., Birman, K., Linga, P., Demers, A., van Renesse, R.: Building an Efficient and Stable P2P DHT through Increased Memory and Background Overhead. In: Kaashoek, M.F., Stoica, I. (eds.) IPTPS 2003. LNCS, vol. 2735, Springer, Heidelberg (2003)
18. Zhuang, S.Q., Zhao, B.Y., Joseph, A.D., Katz, R.H., Kubiatowicz, J.D.: Bayeux: An Architecture for Scalable and Fault-Tolerant Wide-Area Data Dissemination. In: Proceedings of The International Workshop on Network and Operating Systems Support for Digital Audio and Video, NOSSDAV (2001)
19. Kubiatowicz, J., Bindel, D., Chen, Y., Czerwinski, S., Eaton, P., Geels, D., Gummadi, R., Rhea, S., Weatherspoon, H., Wells, C., Zhao, B.: OceanStore: An Architecture for Global-Scale Persistent Storage. In: Proceedings of the international conference on Architectural support for programming languages and operating systems (ASPLOS), vol. 28 (2000)
20. Castro, M., Druschel, P., Kermarrec, A., Rowstron, A.: SCRIBE: A Large-Scale and Decentralized Application-Level Multicast Infrastructure. IEEE Journal on Selected Areas in communications 20(8) (2002)
21. Germanus, D., Khelil, A., Suri, N.: Increasing the Resilience of Critical SCADA Systems Using Peer-to-Peer Overlays. In: Proc. of The 1st International Symposium on Architecting Critical Systems, ISARCS (2010)
22. Dongni, R., Li, Y.T.H. and Chan, S.H.G. On reducing mesh delay for peer-to-peer live streaming
23. Guillaume, J.L., Latapyand, M., Magnien, C.: Comparison of Failures and Attacks on Random and Scale-Free Networks. In: Anderson, J.H., Prencipe, G., Wattenhofer, R. (eds.) OPODIS 2005. LNCS, vol. 3974. Springer, Heidelberg (2006)
24. Dinger, J., Hartenstein, H.: Defending the sybil attack in p2p networks: taxonomy, challenges, and a proposal for self-registration. In: Proceedings of The First International Conference on Availability, Reliability and Security, ARES (2006)
25. Singh, A., Castro, M., Druschel, P., Rowstron, A.: Defending against eclipse attacks on overlay networks. In: Proceedings of the ACM SIGOPS European Workshop, EW (2004)
26. Saxena, N., Tsudik, G., Yi, J.H.: Admission control in peer-to-peer: design and performance evaluation. In: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, SASN (2003)
27. D'Antonio, S., Romano, L., Khelil, A., Suri, N.: INcreasing Security and Protection through Infrastructure REsilience: the INSPIRE Project. In: Proceedings of The Workshop on Critical Information Infrastructures Security, CRITIS (2008)
28. Cohen, E., Shenker, S.: Replication Strategies in Unstructured Peer-to-Peer Networks. In: Proceedings of the 2002 ACM SIGCOMM Conference (2002)

Improving Wireless Sensor Network Resilience with the INTERSECTION Framework

Gareth Tyson, Adam T. Lindsay, Steven Simpson, and David Hutchison

Computing Department, Lancaster University
Lancaster, LA1 4WA, UK
{g.tyson,atl,ss,dh}@comp.lancs.ac.uk

Abstract. This paper investigates the INTERSECTION Framework's ability to build resilience into Wireless Sensor Networks. The framework's general details are examined along with general approaches to protection against misbehaving WSN nodes. Three different approaches to remediation were implemented and tested on a TinyOS network for their different operating characteristics.

Keywords: WSN, remediation, sensor networks, distributed systems.

1 Introduction

Many aspects of computing involve the need to intelligently and dynamically select between many possibilities to achieve optimisation. One example of such a field is *network resilience*. Modern networks are exposed to a wide-range of possible security attacks that can be remediated through a variety of mechansisms. The suitability of these mechanisms, however, can dynamically vary over time and therefore the optimality of a decision can often only be resolved at attack-time. Design-time 'best practice' approaches to defending against such attacks therefore become ineffective.

The INTERSECTION framework [1] was created to address these concerns. It offers an extensible, modular and dynamic remediation service for dealing with security and resilience issues in networked infrastructure. The framework executes a control loop that takes distributed network observations that fuel the deployment of optimisations for handling security threats. Importantly, decisions are taken dynamically (and autonomously) to reflect current operating conditions as well as higher level policy concerns. This framework has successfully been deployed in a range of environments, including Internet service providers and satellite networks. However, one field that provides a more significant challenge is the deployment of these principles within *wireless sensor networks*.

Wireless sensor networks have distinct requirements with respect to resilience due to their high vulnerability and limited defence capabilities. This stems from their often physically open deployment alongside their limited processing and battery capacity. These design concerns result in the frequent inability to utilise sufficiently sophisticated techniques to defend against security threats. Further,

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 415–426, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

even ‘best practice’ approaches can vary in their effectiveness, making the possible overheads they introduce unnecessary.

This paper details the application of the INTERSECTION framework in the realm of wireless sensor networking. To achieve this, a case-study has been chosen which we term *the misbehaving node*. This anomaly consists of a mis-function where a node is in an operating state that negatively affects other nodes in the network. This could be through a malicious reconfiguration or a hardware-related malfunction. Due to resource restrictions, many WSN communications protocols are insecure and susceptible to such anomalies. Further, the nature of the anomalous behaviour can vary greatly between different networks. As such, we use this to highlight the advantages of utilising the INTERSECTION framework. We present three possible remediations to the attack before investigating them using both quantitative and qualitative means.

2 The INTERSECTION Framework

This section details the INTERSECTION security framework and its use in securing wireless sensor networks.

2.1 Overview

The INTERSECTION framework is a security framework developed as part of the EU FP-7 INTERSECTION project. It offers a holistic approach to network security management and strives towards the autonomic defence of network infrastructure. It works, in essence, on a control-loop through which it consumes statistics, detects attacks and then deploys remediations. This chain of operation is fuelled by the ability to configure each instantiation with rules defined by its operating conditions and higher level policies. It was informed in no small part by the ResiliNets initiative [2].

The framework has been tested and deployed within a range of network technologies ranging from traditional IP infrastructure to satellite networks. This paper, however, focusses on the framework’s use in the field of wireless sensor network (WSN) security. As such, a subset of its relevant functionality is now detailed; readers are directed to [1] for a full architectural overview.

2.2 Probes

The first component used in the INTERSECTION framework’s WSN support is the *probe*. A probe is a entity that resides in the network with the task of collecting statistics. There are no predefined set of probes that must be inserted into the network. Instead, they can be dynamically added and removed.

Within a WSN deployment the probe is most likely to reside at the sink. This allows the probe to collect important statistics such as packet rate, packet size packet contents etc. Alongside this, probes can also exist within the network on one or more sensor nodes. These nodes, however, will usually be required to forward their data through the sink and therefore can be considered as constituents of the probe at the sink. Each node collects statistics – reception rates of packets from each of its neighbours, implemented as an additional sensor value – and forwards them to the sink. The sink then collects this information and passes it to the rest of the framework using IPFIX [3] messages.

2.3 Detection Engine

The second important component is the *Detection Engine*. This is responsible for processing statistics gathered by the probes. It is a pluggable component that resides (by default) at a remote location. It receives IPFIX messages from probes and uses detection techniques to detect any attacks [4].

If an attack is detected, the Detection Engine generates a message containing the identifier of the attack alongside any important parameters (e.g. the source). Messages are formatted using IDMEF [5] which is a standard XML message format for describing network intrusions. This IDMEF message is then forwarded to the Remediation Engine using a pub/sub middleware (e.g. JMS [6]).

2.4 Remediation Engine (PITS)

The third important component is the *Remediation Engine*; the current implementation of this is called PITS (Pluggable Intrusion Tolerance System) [7]. PITS is a constituent element of the INTERSECTION framework that is responsible for deploying, revoking and managing remediation mechanisms within the network. Remediation contrasts with traditional 'best practices' as it is a *temporary* measure to resolve a particular runtime problem. As such, it incurs a specific cost that must be weighed against its benefits.

PITS listens for alerts from the Detection Engine regarding any attacks occurring under its jurisdiction. This is identified by the parameters provided within the IDMEF message.

Once the alert is received, the Remediation Engine is responsible for selecting the best remediation for the event. This is based on extensible policy rules that are associated with each Remediation Engine that reflect a cross between policy, capabilities, and run-time information on the anomaly. Each remediation is implemented as a pluggable component that can be dynamically instantiated at a remote location to counteract a given attack. The Remediation Engine therefore deploys these properly configured components to these remote locations (termed Remediation Points) on demand. PITS can reside at any accessible location in the network, but in this scenario, PITS is deployed at the WSN access point.

2.5 Remediation Points

The fourth important component is the *Remediation Point* (RP). These are programmable entities within the INTERSECTION framework that reside at strategic locations in the network. For instance, in an IP network various border routers are likely to be Remediation Points. RPs listen for reconfiguration requests from the Remediation Engine, informing them to perform specific actions. Concretely, they receive requests to instantiate pluggable remediation components that can counteract some observed attack. Requests are structured as XML documents that stipulate which components to instantiate, how to connect them and any required parameters.

When the reconfiguration request is received, the Remediation Point begins to perform the remediation. Alongside this, it also collects statistics that can be fed back to the Detection and Remediation Engines so that they may signal the withdrawal of the remediation. Current WSN operating systems and software do not typically support dynamic reconfiguration to this extent and therefore any remediation functionality must be statically deployed on each node. This functionality is then invoked using authenticated protocol messages sent by the sink (connected to a more powerful machine). We are currently also investigating the use of emerging dynamic WSN operating systems such as Lorien [8] which would offer the necessary capabilities.

3 The Misbehaving Node

This section details the anomaly of interest with the intent of highlighting the potential of the INTERSECTION framework.

3.1 Scenario

The anomaly investigated in this paper is termed the *misbehaving node* scenario. The scenario is an by-product of lightweight – and insecure – configuration protocols utilised by simple wireless sensor network deployments, such as the Collection Tree Protocol [9].

Many sensor networks use remote configuration protocols that allow nodes to be configured and reconfigured dynamically post-deployment. This has many benefits, specifically allowing a large number of nodes to have their behaviour modified without the need for staff to manually re-program all nodes. We term this method of dynamic re-configuration a *control protocol.*

Control protocols are generally application specific and designed by the developer to match their exact needs. These needs can vary between different deployments; common examples are sensor sampling rate, remote update rate and which sensors to probe.

There are a countless ways for a wireless sensor node to misbehave in the face of hardware damage or malicious or negligent reconfiguration. To provide focus, however, we address one particular type of anomaly – one that adversely affects the well-being of the sensor network as a whole – termed *packet injection.* This occurs when the misbehaving node has an increased data transmission rate. This is dangerous as all packets received by the root appear valid, as if they had been generated by an existing member of the network. This has three effects:

- Denial of Service: Nodes within the network will have an increased routing load. This can result in greater packet loss and delay.

- Battery Drain: The increased routing load will result in high battery consumption from all nodes ‘downstream’ from the anomaly.
- Untrustworthy data: The increased transmission rate may cause spurious or untrustworthy data to be entered into the system.

3.2 Intuitive Solutions

A number of intuitive approaches exist to remediate against this anomaly. The first would be *encryption*; this would involve using encryption to authenticate control messages. This is feasible in some situations, however, such authentication algorithms may take up to minutes to process. Depending on the frequency of control messages this can be considered too long for many applications. More recent advances can reduce that to seconds [10], though at greater expense in cost and energy. Further, the complexity of using such algorithms could be considered to be inappropriate by many developers that do not see their sensor networks as susceptible enough to such anomalies to justify the increased ongoing cost.

The second solution would be to remove the usage of the control protocol, therefore eliminating the vulnerability. Once again, this is a possibility, however, this cannot be performed if the control protocol is integral to the network's correct operation. Alternatively, only a subset of the protocol could be disabled; this, however, only mitigates the problem – it does not solve it.

The final intuitive solution that we consider is placing hard coded limitations on the protocol's parameters. This would prevent malicious reconfigurations that emit values that lie outside a certain threshold (e.g. X must be > 10 and < 20). This, once again, would mitigate the problem but not solve it. Also, in many situations the defence could be worked around by making small variations on many nodes rather than one large variations on a few nodes.

4 WSN Deployment

This section details three pluggable remediation mechanisms that are utilised by the INTERSECTION framework to handle the security problems outlined in Section 3. Each can be dynamically selected based on the environment in which the WSN and attack(s) operate in.

4.1 INTERSECTION Configuration

As discussed in Section 2, the framework consists of four primary elements: probes, reaction engine(s), remediation engine(s) and remediation point(s). Within the current WSN setup, these are deployed as follows:

- Probes: Each sensor node acts as a probe. It counts the number of packets it receives from each of its neighbours then periodically forwards this information to the root. The root also acts as a probe by counting the number of received packets. Both sets of information are then forwarded to the Reaction Engine.

- Reaction Engine: One Reaction Engine exists in the setup. This is located at a remote host that has connectivity with the root.
- Remediation Engine: One Remediation Engine operates at the root. This is configured with policy rules based on the particular WSN.
- Remediation Point: The Java implementation of the Remediation Point is co-located with the Remediation Engine. It interacts with WSN using a serial connection to the root through which is can forward messages through. Each sensor node also has remediation functionality that can be invoked by the Remediation Point using a authenticated protocol.

4.2 Remediation Mechanisms

To resolve the case-study attack detailed in Section 3, three remediations are proposed. These are embodied in pluggable components that can be selected and instantiated at the Remediation Point located at the WSN root. Once instantiated, they disseminate an authenticated protocol messages into the WSN informing a particular node to instantiate a remediation strategy. These possible strategies are now detailed.

Node Re-Initialisation. This is the simplest remediation available as it involves no network reconfiguration. Instead, the remediation mechanism simply sends a reset message to the compromised node, informing it to return to its default configuration. Subsequently, it should return to its normal rate.

Route Around. The second approach remediates against the possibility that a node cannot be reinitialised. This occurs when an attacker repeatedly misconfigures the node by periodically sending malicious control messages. Therefore, whenever the node is reinitialised, the attacker re-sends the command telling the node to increase its sending rate.

The INTERSECTION remediation for this attack is to broadcast a reconfiguration message to all nodes. This message informs the recipients to stop forwarding messages from the compromised node, effectively shunning the anomaly. Subsequently, the node's messages are limited to one hop in the collection tree.

Node Shutdown. The third approach remediates against the situation in which the compromised node is sending at such a high rate, that its immediate neighbours (within radio range) are having their batteries depleted by processing the messages. Therefore, the compromised node is still having a significant impact on a subset of the nodes. To remedy this, all nodes within radio range of the compromised node are shutdown so that it remains quarantined without the necessity to filter its messages. These node subsequently operate with resume timeouts so that the nodes turn resume operation after a given period. If the attack is still taking place and the circumstances haven't changed, these nodes can then be shutdown again.

5 Evaluation

This section evaluates the INTERSECTION framework's ability to provide on-demand remediation in a wireless sensor environment. The key aim of the evaluation is to examine the framework's ability to select and deploy appropriate remediations based on its operating context. To this end, the performance and overhead of each of the remediations are examined. Following this, each strategy is investigated to find its suitability in different situations.

5.1 Methodology

The INTERSECTION framework has been implemented in Java alongside the three remediation mechanisms by modifying the CTP [9] implementation in TinyOS [11]. Using this modified CTP, a simple sensor sampling application is setup in the TOSSIM simulator. A 64 node grid topology is constructed with each node spaced 2 metres apart with a noise floor of -105 dBM. Every minute, each node sends a sensor reading to the sink. The attack begins after 60 minutes; this attack involves a single node's sending rate increasing from 1/min to 1200/min. For the purposes of this evaluation, an alert simulating detection of the anomaly is generated after 4 minutes, and the chosen remediation is deployed.

5.2 Evaluation of Remediation Mechanisms

As shown in Section 4, there often exist multiple approaches to correcting an anomaly. Subsequently, to make an informed decision about remediation strategies it is necessary to understand the behaviour and characteristics of the available remediations. This section now explores the performance and overhead issues of each of the three possible remediations detailed in this paper.

Performance. To evaluate the performance of the remediation mechanisms we use the packet reception rate. This can simply be defined as the number of packets received by the CTP root over a given period of time. Any deployed sensor network will have upper and lower bounds on this reception rate; subsequently, extended periods of operation outside of these limits indicates an anomaly. Figure 1 shows the reception rate at the root when operating with the three remediation strategies. It can be observed that after 60 minutes, the attack begins with a dramatic increase in the reception rate. The detection mechanism alerts the INTERSECTION framework 4 minutes after the attack starts and subsequently a remediation is deployed.

The *re-initialisation* remediation is the most effective with an immediate drop in the reception rate. Further, the network is returned entirely to its previous state without any drops below the original reception rate.

The *route around* mechanism also has similar results; a notable difference, however, is that this remediation involves severing the compromised node from the network. Subsequently, its data is lost and the reception rate drops to reflect this loss of data.

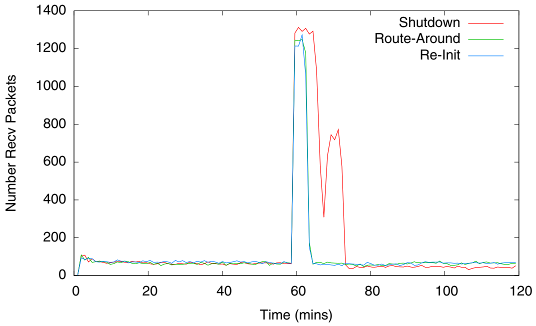


Fig. 1. Packet Reception Rate at Root with Different Remediations

Table 1. Reception Rates Before and After Remediations (per min)

Remediation	Before	After	Diff
Re-Init	68	68	0
Route Around	61	58	3
Shutdown	65	43	22

The *shutdown* remediation has the most significant effect on the reception rate. Once this remediation is executed, the nodes that neighbour the compromised node begin to shutdown. This happens progressively as the dissemination protocol contacts each node. As it is necessary to contact a greater number of nodes (18) than previously, the reaction of this remediation is slower. Once the remediation begins to take effect there is a sharp fall in the reception rate. However, as not all neighbouring nodes have been shutdown yet, it becomes possible for the compromised node to recover its route to the sink by using alternative hops. This results in an increase, yet again, in the reception rate. This, however, is short-lived as the rest of the neighbours soon receive the remediation command, thereby fully quarantining the compromised node from the rest of the network. Once the remediation has taken effect, the reception rate can be seen to be well below the previous level due to the number of network members that cease to send their sensor data.

A summary of the results is shown in Table 1. This shows the average reception rate (per minute) both before and after the remediations have been put in place. It can be seen that the re-initialisation remediation has little effect on the reception rate. In contrast, the route around and shutdown remediations decrease the sending rates. This results in fewer sensor samples being received.

Overhead. A vital consideration when deploying a remediation is its overhead. A remediation that is not associated with an overhead should be considered a best practice that should be under constant deployment. Therefore, generally the overhead of a remediation forms the foundation for the selection criteria. This section now explores the overhead of the three remediations investigated.

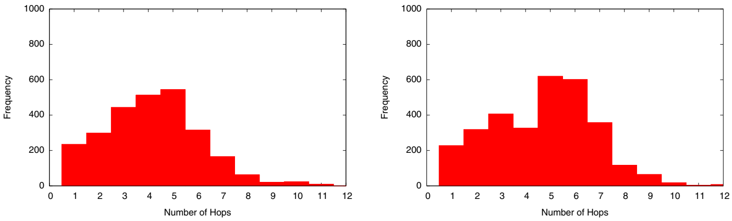


Fig. 2. Histogram of Routing Hops (i) before and (ii) after Route-Around remediation

Two forms of overhead are identified; the first is an increased number of hops between the clients and the root. The second is an increased delay between the clients and the root.

The *re-initialisation* remediation is, unsurprisingly, the optimal mechanism in terms of overhead. Once the attack is detected it is simply a matter of sending a single message to the compromised node. Following this, the sending rate returns to normal and no further overhead is suffered.

In contrast, the *route-around* remediation has a larger overhead as it involves the modification of routing behaviour. Figure 2 provides a histogram of the number of hops both before and after the remediation is put in place. After executing the remediation within the experiment, 28 nodes suffer from an increased number of hops. On average, these nodes witness an increase of 1.2 hops. This subsequently means that the network will suffer from an increased level of battery consumption as the routing process is spread over an increased number of nodes. Despite this, there is little discernible effect in terms of the delay observed within the network; this can be attributed to the ease at which the nodes can route around the single failure.

The *shutdown* remediation has the greatest overhead because it creates the greatest disruption in the network. Within the experiment, 18 nodes (28%) are within range of the compromised node; subsequently, these members of the network must be shutdown to quarantine the attack and preserve their batteries. Figure 3 shows the effect that the remediation has on the number of hops. It can be observed that this has a significant impact on the number of hops a node requires to contact the root. Before the remediation, the mode average of hops is 5, however, this increases to 7 after the remediation is put in place. This increase is driven by the 28 nodes (44%) in the network which find their route(s) compromised by the remediation. These nodes witness a mean increase of 2.3 hops. Globally, this results in the mean average increasing from 4.9 hops to 6.2. Unlike, the route-around remediation, however, this increase does result in a noticeable change in delay. Before the remediation, the nodes have an average delay of 733 ms, however, after the remediation this increases by 137 ms to 870 ms.

5.3 Analysis of Remediation Characteristics

The previous quantitative investigation has exposed the differences between the behaviour of each remediation strategy. Despite their collective ability to resolve

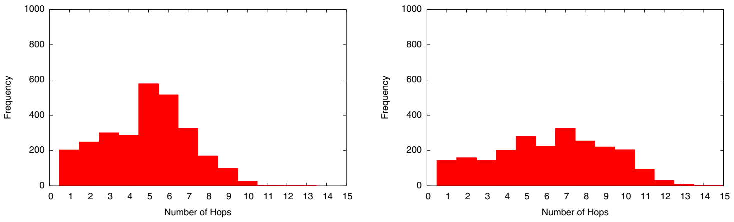


Fig. 3. Histogram of Routing Hops (i) before and (ii) after Shutdown remediation

the attack, it is evident that there are different advantages and costs related with each. This section now explores these with a mind to ascertaining their suitability in different circumstances.

Re-Initialisation Remediation. The first remediation works on the basis that the anomaly is a ‘one off,’ so that the misbehaving node can be returned to normal with a software reset, and there is no malicious party that will reconfigure the node again. If these are not the case, the remediation is ineffective because every time the re-initialisation takes place, the anomaly will reoccur. Despite this, it is by far the most effective as it capable of returning the network to completely normal operating conditions. The performance and overheads of the re-initialisation remediation are therefore the most attractive.

This remediation should always be the first to be attempted as it offers the greatest utility at the lowest cost. However, its deployment must also be performed alongside continued monitoring. If it is unsuccessful in its task then the remediation must be withdrawn and replaced with an alternative.

Route-Around Remediation. The second remediation is a network level solution that prevents the misbehaving node from polluting the network with an increased packet rate. Unlike the previous remediation, this remediation is resilient against the continuing presence of the attacker. However, this also results in the loss of data from the compromised sensors. Subsequently, if the data is highly important and the network can handle the increased traffic, it could be considered a superior option to allow the node to continue sending.

This remediation should be the default choice after the failure of the re-initialisation remediation as it will ensure that the compromised node is quarantined. It is highly feasible in most circumstances and provides the best performance when operating with a continually present attacker. However, because the compromised node remains in contact with the other nodes, there can be a notable level of battery consumption due to their new function as filters. This largely depends on the sending rate and range of the compromised node.

Shutdown Remediation. The third remediation is an extreme solution that can be taken if the compromised node's sending rate is adversely affecting those around it. It works by shutting down all peers that are within the transmission range of the offending node. This therefore maintains quarantine whilst also ensuring that the surrounding nodes do not have to expend energy filtering the

Table 2. Overview of Remediation Strategies

Factor	Re-init	Route Around	Shutdown
Effectiveness	Low	High	High
Increased Delay	None	Limited	High
Increased Hops	None	Limited	High
Loss of data	None	Limited	High
Increased Battery	None	None	Reduced

Algorithm 1. Default Algorithm for Remediation Selection

```
success = deployReInit();
if success == true then
    return SUCCESS;
else if (sensor data not critical || high replication in network) && battery life important then
    deployShutdown();
else
    deployRouteAround();
end if
```

messages they receive. This thereby lowers the battery consumption of the neighbouring nodes so that they can be restarted at a later date once the offending node has been removed.

Shutdown has the side-effect of removing the relevant nodes' sensor data from the system. This can be considered a necessary sacrifice (as defined by policy) if the human interception time is extended or if the data is not vital (e.g., it can be covered by other sensors). The selection of the shutdown remediation is therefore largely based on environmental and application issues that would indicate it is acceptable to shutdown the nodes in favour of maintaining their batteries.

Summary. It is evident that the three remediation mechanism are suitable for deployment when operating in different conditions. Table 2 provides an overview of their differences. To formalise these results, Algorithm 1 also details the selection policy. In essence, the re-initialise remediation should *always* be tried first. If this fails, one of the other two remediations should be deployed. If the sensor data is not critical or, alternatively, there are many sensors that can replace the lost ones, the next approach is to perform the shutdown remediation (assuming battery preservation is important). However, if these pre-requisites are not fulfilled then the policy default is to use the route around remediation.

6 Conclusion

This paper has outlined the application of the INTERSECTION framework in the domain of wireless sensor networking. The *misbehaving node* wireless sensor anomaly has been detailed alongside a set of three possible remediations.

This has then been placed in the context of the INTERSECTION framework to investigate the advantages of allowing such a security system to dynamically select which remediation to deploy based on environmental conditions and higher level policy concerns. Through this, it has been shown that the three remediations – re-initialisation, route-around, and shutdown – possess greatly different characteristics and, as such, are not uniformly suitable for all situations.

There are a number of possible areas of future work. It is necessary to investigate the usage of the INTERSECTION approach with a range of different security threats. Different WSN routing protocols should be investigated for their applicability to the lightweight and flexible remediation strategies we examined in the context of the CTP protocol. Finally, the research would be greatly strengthened with a more ecological investigation into varied range of actual environmental deployments.

Acknowledgements. This research is funded by the EU INTERSECTION Project under grant agreement no. 216585. The authors thank Utz Roedig for his feedback on early drafts.

References

1. D'Antonio, S., Romano, S.P., Simpson, S., Smith, P., Hutchison, D.: A Semi-Autonomic Framework for Intrusion Tolerance in Heterogeneous Networks. In: Hummel, K.A., Sterbenz, J.P.G. (eds.) IWSOS 2008. LNCS, vol. 5343, pp. 230–241. Springer, Heidelberg (2008)
2. Sterbenz, J.P., Hutchison, D.: Resilinets wiki, `http://wiki.ittc.ku.edu/resilinets_wiki/`
3. Claise, B.: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information. Number 5101 in RFC. IETF (January 2008)
4. Coppolino, L., D'Antonio, S., Esposito, M., Romano, L.: Exploiting diversity and correlation to improve the performance of intrusion detection systems. In: International Conference on Network and Service Security, Paris, France (June 2009)
5. Debar, et al.: Ietf intrusion detection exchange format working group. Internet Draft. IETF (2004)
6. Sun: Java Message Service (JMS), `http://java.sun.com/products/jms/`
7. Simpson, S.: Pluggable Intrusion Tolerance System (PITS), `http://www.activenet.lancs.ac.uk/pits/`
8. Porter, B., Coulson, G.: Lorien: a pure dynamic component-based operating system for wireless sensor networks. In: 4th International Workshop on Middleware Tools, Services and Run-Time Support for Sensor Networks (MidSens 2009), Urbana Champaign, Illinois, USA, pp. 7–12. ACM, New York (2009)
9. TinyOS Network Working Group: The Collection Tree Protocol (CTP), `http://www.tinyos.net/tinyos-2.x/doc/html/tep123.html`
10. Szczechowiak, P., Oliveira, L., Scott, M., Collier, M., Dahab, R.: NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks. In: European Conference on Wireless Sensor Networks (EWSN 2005), Bologna, Italy (2005)
11. TinyOS Alliance: TinyOS, `http://www.tinyos.net/`

Trust Management in Monitoring Financial Critical Information Infrastructures

Giorgia Lodi[1], Roberto Baldoni[1], Hisain Elshaafi[2], Barry P. Mulcahy[2],
György Csertán[3], and László Gönczy[3]

[1] University of Rome La Sapienza, Italy
`{lodi,baldoni}@dis.uniroma1.it`
[2] Waterford Institute of Technology, Ireland
`{helshaafi,bmulcahy}@tssg.org`
[3] OptXware Research&Development Ltd, Hungary
`{csertan,gonczy}@optxware.com`

Abstract. The success of Internet-based attacks and frauds targeting financial institutions highlights their inadequacy when facing such threats in isolation. Financial players need to coordinate their efforts by sharing and correlating suspicious activities occurring at multiple, geographically distributed sites. CoMiFin, an European project, is developing a collaborative security framework, on top of the Internet, centered on the Semantic Room abstraction. This abstraction allows financial institutions to share and process high volumes of events concerning massive threats (e.g., Distributed Denial of Service) in a private and secure way. Due to the sensitive nature of the information flowing in Semantic Rooms, and the privacy and security requirements then required, mechanisms ensuring mutual trust among Semantic Room members (potentially competitive financial players) must be provided. This paper focuses on the design and preliminary implementation of a trust management architecture that can be configured with trust and reputation policies and deployed in Semantic Rooms.

Keywords: Financial critical infrastructures, collaborative environment, trust, reputation, monitoring, trust metrics.

1 Introduction

Context and Motivations. An increasing amount of financial services are provided over publicly accessible communication mediums such as the Internet. As a result, those services and their supporting IT infrastructures are exposed to a variety of coordinated and massive Internet-based attacks and frauds [1], [2], [3], [4] that cannot be effectively handled by any single financial organization. Therefore, financial institutions need to coordinate their efforts in order to offer the computational power and collective information assets that are capable of discovering and containing those threats [5]. Let us consider as an example large-scale stealthy scans. An attacker performs such scans against financial institutions with the aim of capturing sensitive information on edge sites of the

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 427–439, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

target institutions, this typically includes reachability and status of specific ports and IP addresses [6]. The outcome of the scan is to create a list of potentially vulnerable hosts. This list can then be exploited by the attacker to compromise such hosts and, as an example, deny the access to hosts' services from customers and/or internal users. Stealthy scans are becoming increasingly sophisticated: they are typically initiated from many geographically dispersed locations simultaneously and target multiple hosts scanned at random [7]. Hence, it is likely that single existing detection systems (e.g., Intrusion Detection Systems), deployed in isolation at individual financial institutions, are incapable of discovering a sufficient number of scans within a predefined time window to identify these events as an attack. Collaborative security environments are, thus, required in order to detect such attacks, as they can be effectively deployed to aggregate and correlate a higher amount of data, coming from multiple financial sources, that collectively show evidence of an attack.

In the context of the EU funded project CoMiFin [8] we are developing a framework that enables the construction of such collaborative security environments centered on the *Semantic Room (SR)* abstraction. An SR allows financial institutions to customize private spaces on top of the Internet for secure data sharing and data processing. SRs have a specific strategic objective to fulfill (e.g., an SR for stealthy scans detection) and are regulated by contracts that specify the set of rights and obligations to be met for being part of them (e.g., security and privacy requirements). Such sharing of information raises trust issues with respect to the information flowing in the SR. Indeed, in this setting, there can exist different types of SRs with different levels of trust requirements. At one extreme there could be SRs formed by financial institutions that trust each other implicitly (e.g., branches of the same bank), and consequently trust the information being processed and shared in those SRs. At the other extreme, there could be SRs whose membership includes participants that are potential competitors in the financial market. In this case, the issue of trusting the information circulating in a semantic room becomes a point of great importance and if this issue is not adequately addressed, the semantic room abstraction will be infeasible as financial institutions will refrain from becoming members of it. Proper mechanisms that ensure a measurable level of trust among SR participants are therefore required.

Contribution. In this paper, we propose the design and preliminary implementation of a trust management architecture that is capable of specifying and communicating trust metrics among distributed SR financial institutions. An example of a trust metric we evaluate is the reputation value associated with each financial institution belonging to an SR. This measure reflects the perceived competence, integrity, and/or behavioural aspects of each financial institution that is providing information to an SR. The reputation value depends on the configuration of the trust algorithm for that metric and the result can be used to weight the quality of information provided thereby increasing or decreasing its significance. The architecture is able to dynamically update the level of trust attributed to participants according to monitored participants' behaviours, undertaken in SRs; this includes compliance with the requirements specified in SR contracts. The design of the architecture is highly flexible and includes the ability to apply multiple trust update policies to SR information flows. In this paper we present a specific policy that dynamically computes at run time the reputation of SR participants based on their monitored behaviours and their reputation in other SRs to which they may belong.

Related work. The need for collaborative systems for coping with the current generation of threats and security attacks is highlighted in a number of works that can be found in the literature (e.g., [5][9][10]). In addition, the need to properly deal with trust in distributed environments in which many distrusting entities can collaborate is emphasized in some recent works (e.g., [11][12]). This highlights just how important it is to ensure a certain level of trust among collaborative entities, especially in contexts where sensitive information must be shared, as in our case.

Reputation management, that is, the combination of first hand experience with third party recommendations to create a feedback loop for determining trustworthiness, has proven to be an integral part of modern trust management systems [13], [14], [15] [16], [17], [18]. These works share a number of similarities with our approach. In all cases, a feedback-based mechanism is utilised in order to assess the reputation of participants in the system. In particular, a local reputation value is used that is analogous to our local history function as described in Section 3.2. In addition, all the works above are applied to P2P environments when computing the reputation of peers for file sharing purposes. Typically, in these P2P systems contracts are not used to regulate relationships among peers; the system is "flat" and the reputation is not controlled and differentiated on the basis of the type and requirements as contractually specified, as in our case.

The rest of this paper is organized as follows. Section 2 presents the Semantic Room abstraction where the trust management architecture can be used. Section 3 describes the design of the trust management architecture. In particular, this Section explains how monitoring SR contracts can impact the level of trust within SRs. Section 4 presents a premilinary implementation of our trust management architecture and finally Section 5 provides the conclusions of the paper.

2 The Semantic Room Abstraction

A Semantic Room is a federation of financial institutions that wish to be grouped together for the sake of information processing and sharing. The partners participating in a specific SR are referred to as the *members* of the SR.

Each SR is associated with a *contract* that defines the set of processing and data sharing services provided by that SR along with the data protection, isolation, trust, security, dependability, and performance requirements. The contract also contains the hardware and software requirements a member has to provision in order to be admitted into the SR. In Figure 1 SR members provide raw data to the SR(s) that they are part of. This data may include real-time data, inputs from human beings, stored data (e.g., historical data), queries, and other types of dynamic and/or static content. Raw data is processed internally by each SR.

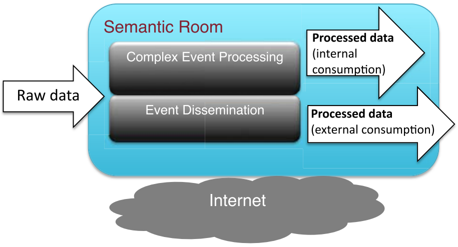

Semantic Room
Complex Event Processing
Event Dissemination
Raw data
Processed data (internal consumption)
Processed data (external consumption)
Internet

Fig. 1. Semantic Room abstraction

The resultant processed data can be used for internal consumption within the SR: in this case, derived events, models, profiles, blacklists, alerts and query results can be fed back into the SR so that the members can take advantage of the intelligence provided by the processing. SR members can, for instance, use these data to properly instruct their local security protection mechanisms in order to trigger informed and timely reactions independently of the SR management. In addition, a (possibly post-processed) subset of data can be offered for external consumption. SR members have full access to both the raw data that the members agreed to contribute by contract, and the data being processed and thus output by the SR. Data processing and results dissemination is carried out by SR members based on the contractual obligations and restricts specified in the SR contract.

In addition to the SR members, there can exist clients of the SR. These clients cannot contribute raw data directly to the SR; however they can be consumers of the processed data that the SR is willing to make available for external consumption (Figure 1).

SRs can communicate with each other. In particular, processed data produced by an SR can be injected into another SR (e.g., through the SR client role described above) as regulated by its contract. The ability for SRs to communicate with one another may enable a composition of multiple services, provided by each individual SR, into higher-level functionalities. For instance, processed data in the SR related to "DDoS attacks on FIs" can be used by a more specialized SR such as "DDoS attacks on banks in a country" whose data can be, in turn, used by the SR related to "DDoS attacks on a specific bank in a specific country" in order to provide partners with richer services (Figure 2).

Figure 2 depicts a hierarchy of SRs in which a member (in the example bank1_Agency1) belongs to more than one SR. The hierarchy structure enabled by the SR abstraction can be effectively used in order to control the level of privacy and security provided by the SR for the information being accessed, shared, and processed inside it. Specifically, in "private" SRs where only members of the same organization participate (in Figure 2 the leaf nodes in the hierarchy) sensitive information, possibly concerning financial transactions, might be fully visible and accessible to the members of that SR. In this case, members trust each other as they belong to the same organization and mutual trust is inherently ensured. In contrast, in large and heterogeneous SRs (e.g., in Figure 2 the "DDoS attacks to FIs" SR), the level of privacy and security specified in the SR contract (in Figure 2 the SLA associated with each SR), and required by FIs for the exchanged and processed information can be significantly different from that

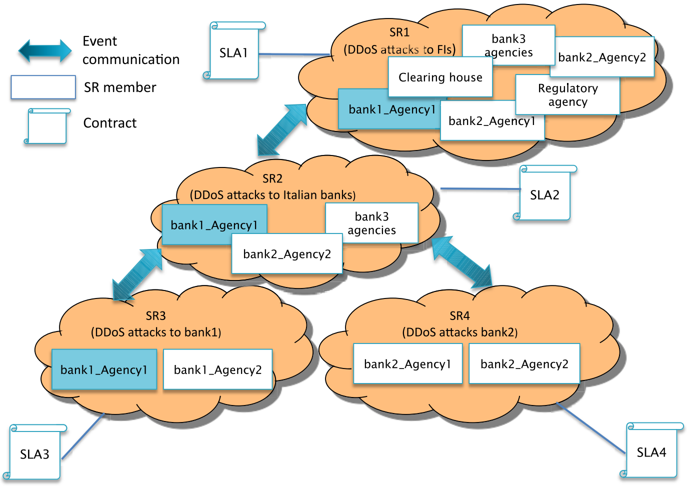


Fig. 2. SR hierarchy and communication

required in the leaf node SRs. This is due to the fact that in large SRs FIs can be potential competitors in the financial market. Competitor FIs may decide to federate despite this in order to take advantage of the intelligence produced by the SR; however, they do require more stringent requirements on the SR members' behaviours before making available their own data to the SR. In these large scale SRs with distrusting members, it is necessary to support the information processing and sharing while guaranteeing mutual trust among members (i.e., while ensuring information trustworthiness). This requirement can be crucial: without any trust guarantees, these SRs might run the risk of not starting up as distrusting participants can be reluctant to provide their own data to them.

The architecture we introduce in the next section is designed so as to meet such trust requirements including an incentive scheme that promotes constructive participation of members.

3 The Trust Management Architecture

We have designed a trust management architecture which stores, monitors, and updates trust levels of SR members based on the behaviours of those members.

Each SR deploys its own Trust Manager (TM) that, in order to monitor those behaviours, interacts with other two main subsystems we have included in our design; namely, the Event Processing and Metrics Monitoring subsystems, and possibly with other TMs deployed in other SRs.

The TM design is highly flexible to include different types of configurations. Authorized administrators can configure (through a web-based interface) a number of parameters related to the way in which the level of trust is computed. In particular, as illustrated in the use case diagram in Figure 3, administrators can set the preferred update policy of the trust management architecture. This policy can be obtained either from an available set of policies (e.g., a policy repository) or from the SR contract where requirements on how the trust is to be computed can be specified (see below). The administrator can also specify the values of constant parameters such as default trust for new members, and trust threshold to be used in order to identify when interested parties are to be notified of changes to a member's trust (note that, also for these parameters, administrators can properly configure the trust management architecture using the value that might be included in SR contracts).

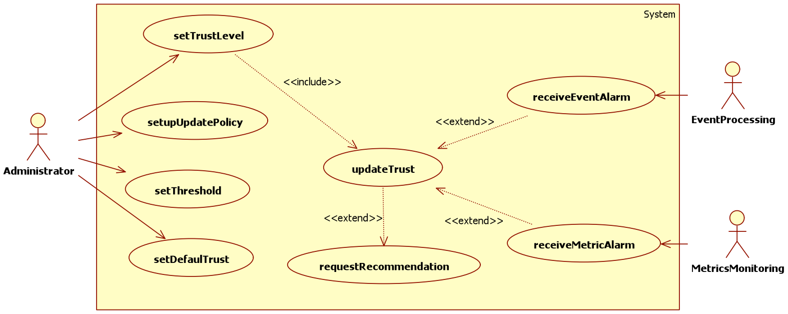


Fig. 3. Trust Management: Main Use Case

Administrators can use those configurations to specify how the initial trust value of each member is calculated and to control how these levels of trust are dynamically computed and updated at run time.

The Event Processing subsystem of an SR interacts with its related TM by sending alarms related to an event of a member that may trigger trust changes. Analogously, the Metrics & Monitoring (MeMo) subsystem of an SR sends alarms to its related TM in case a change in the SR metrics evaluation (e.g. SLA violation/adherence) for a member occurs, as this change can affect other SR members' trust in that member. Additionally, the Event Processing subsystem uses notifications of the trust levels from the TM in order to filter the events based on the sources of those events. For example, events originating from a member with a low trust level might be ignored or assigned to a low priority. Since trust itself is one of the metrics that the system monitors, the MeMo subsystem receives trust updates so that it can monitor the adherence to the SR contract's trust requirements in the same way as it does for the other SR contract metrics such as security, performance, dependability, etc.

Finally, note that it may be possible for the trust management architecture to calculate the trust for a new SR member by asking recommendations related to that member to other SR's TMs. As depicted in Figure 2 a member can belong to more than one SR and the interactions among TMs of different SRs can be required in order to obtain information on the trust levels of that member in different SRs. In general, this approach helps to build reliable trust information on the members by considering their behaviours in many SR collaborative environments.

3.1 SR Contract Monitoring for Trust Management

As previously highlighted trust is a crucial requirement in both the design and operation phases. Trust management in the operation phase utilizes a control algorithm that takes decisions based on trust metric values, which are provided by a metrics monitoring system of the SRs.

Figure 4 shows the general metrics monitoring architecture used in Semantic Rooms. The purpose of the Metrics & Monitoring (MeMo) is to continuously measure and present the status information of services and resources and to generate notification for other components in case of undesired status changes (e.g. SR contract violations).

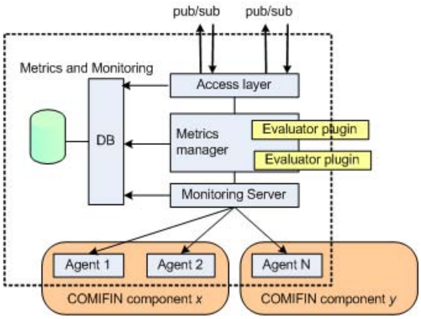


Fig. 4. MeMo architecture

Trustworthiness monitoring can refer to various levels of a system architecture. Typically, high level trust metrics are composed of low-level indicators (number of false alert messages, number of viruses found, number of lost messages, etc.). These can be measured by typical system monitoring tools (Monitoring Server), such as Nagios [19] or Tivoli Monitoring [20], which have good tool support for measurement of IT component parameters by using low-level sensors or agents (Agent 1..N); however, no sophisticated evaluation methods are offered. Therefore, a plugin-based monitoring architecture is designed which allows for plugging-in mathematical tools, rule engines, Complex Event Processing facilities or even other system components such as the Trust management architecture to be used as sophisticated metrics evaluator in the system. Our purpose is to separate SR specific evaluation (e.g. detection of domain-specific DDoS attacks) from infrastructure level monitoring.

Resource level monitoring settings (i.e. placement and configuration of sensors/agents) are generated on the basis of the SR contracts. As the resource pool (and therefore the monitoring requirements) of an SR may change frequently, the monitoring configuration is maintained in a model-based way to adapt sensor/agent setups quickly.

In a *plugin-based monitoring architecture* the TM is used as a plug-in with enhanced trust calculation features. The trust maintenance algorithm will be implemented in the TM while MeMo keeps track of system status information both for low-level security metrics and trust values computed by the TM.

MeMo offers both a *query functionality* and a *publish/subscribe middleware interface* to forward measurement data. This supports a scalable, distributed management architecture for SRs, e.g., security alerts are available for both the components managing the SR and the TM which updates trust metrics.

3.2 Pluggable Trust Policies: A Reputation Framework

We have designed the trust management architecture in order to be configured with different trust policies. In this paper, we focus on a policy that allows us to update the reputation of an SR member at run time. Specifically, we consider here the distributed system depicted in Figure 2 in which an SR member can be involved in more than one SR. As stated above, SRs are regulated by contracts, which we call SLAs from now on; each SLA defines different QoS requirements for which SR members are willing to pay. These requirements can include in which way reputation of members can be computed. In particular, SLAs might specify an initial reputation value (see below) and the functions that are used to compute and update it according to the behaviours of SR members within SRs.

The reputation defined into an SLA can be used as input for other SLAs, thus enabling links among SLAs and, consequently among SRs. The binding among SR SLAs permits different SR members to take advantage of the knowledge on a specific member reputation in other SRs in order to enforce their trust in it and build, as previously mentioned, reliable levels of trust of the members. This knowledge can be crucial in some cases as it might be used for also determining how fast or slow can the reputation judgement towards that SR member be changed. For example, if an SR member does not always behave correctly in the eyes of the other members in the same SR, its reputation in other SRs can count more and influence the final reputation evaluation.

Owing to this scenario, our reputation policy works as follows. It uses the trust parameters included in the SR SLA (e.g., the rules for determining the reputation). Thus, let *sr* be an SR member involved in more than one SR; we claim that in general its reputation is a function that can be defined as in 1:

$$R_{sr_j} = f(history_j, \{R_{sr_i}, ..., R_{sr_k}\} \setminus \{R_{sr_j}\}) \quad (1)$$

$$\text{where} \quad i, j, k \in \{SR1, SR2, SR3, ...\}$$

To compute the reputation, two principal elements are taken into account: (i) the behavior of *sr* in an SR; we call it *local history* i.e., the evaluation of the *sr*'s actions carried out in the SR, (ii) and the reputation that *sr* has in other SRs in case bindings among SLAs are enabled. Note that, if more than one bind exists with other SRs, the reputation function above is able to take into consideration all the reputation functions derived by the linked SRs (what we have called above recommendations).

The local history is a function that is computed, as in case of 1 above, by our policy as follows:

$$history_j = g(init\_rep\_value, [facts_1(sr), ..., facts_k(sr)]) \quad (2)$$

$$\text{where} \quad j \in \{SR1, SR2, SR3, ...\}$$

In other words, the local history is defined by considering an initial reputation value associated with an SR member, and an evaluation of the actions performed by *sr* over the entire duration of the SLA (we call these evaluations *facts* in formula 2). These facts are the input of a feedback-based mechanism through which other SR members belonging to the SR can judge the *sr*'s behavior based on the facts they have observed in that SR. Note that the facts are determined on the basis of the SR contract monitoring carried out by the MeMo subsystem. The result of the monitoring triggers interactions between MeMo and TM so that TM can determine accordingly the behaviours of an SR member.

The initial reputation is a value in the range of [0,1] and represents the initial credibility of the member in the eyes of the other members. This credibility can be influenced by many factors: a previous business experience with the member, the type and the quality of service the member supply to the SR. For instance, we might think that some SR members have a previous long running business relationship with a specific member with which are part of an SR; in this case their initial reputation judgement towards that member can be high; that is, close to 1; in contrast, there can be other SR members that do not have any previous business experience with that member so that they can be reluctant to consider it credible, and wish to evaluate its behavior in the SR in order to define its reputation.

The initial reputation value is then dynamically adjusted at run time by the local history function according to the judgements the SR members express on the specific *sr*'s actions.

4 Trust Manager Design and Implementation

Figure 5 depicts the class diagram of the TM and the subsystems with which it interacts. This preliminary design is based on the architecture described above.

Trust is an object that has a number of attributes including the trust level or the score of the member, the recency, and the confidence of the trust. The recency indicates how recent the trust level is. This allows trust services consumers to determine how reliable the trust level is, and it is useful for update operations as older trust values can be considered less important. Trust confidence ranges between 0 and 1. It is calculated based on the source of the trust value i.e. based on the experience or local history (more confidence) vs. recommendations (less confidence) and the number of trust updates. The more trust is updated, the more the confidence value.

MeMo and Event Processing subsystems subscribe to updates on the trust values and the TM receives metrics and events trust alarms from MeMo and Event Processing, respectively, that it uses in order to update members' trust levels.

The sequence diagram in Figure 6 depicts the use case resulting from an interaction with the MeMo subsystem described above. Specifically, the MeMo sends an alarm to the TM. The alarm triggers a trust update: existing trust is loaded and the configured update policy can be applied in order to update the trust.

If we refer to the pluggable policy described in Section 3.2 the trust can be updated by two f and g functions we have used in our current implementation.

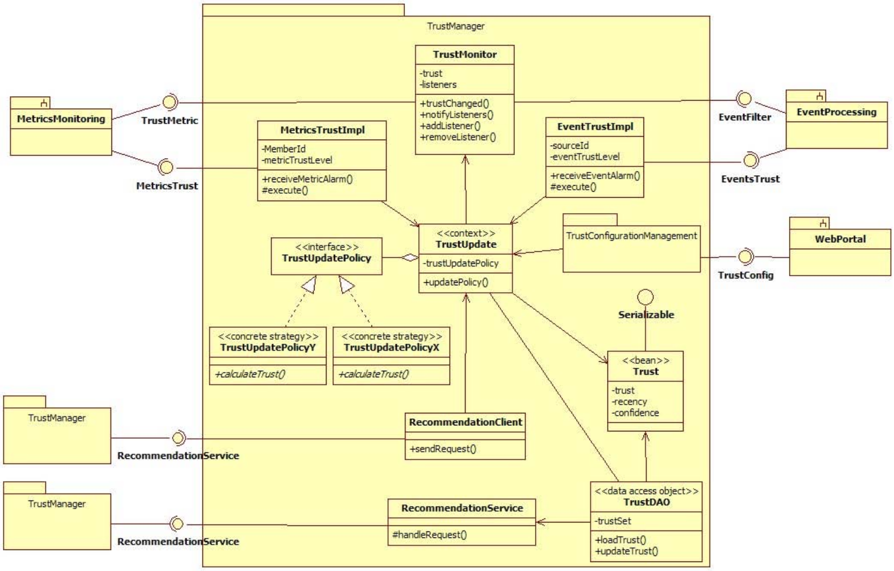


Fig. 5. Trust Management Architecture: Class Diagram

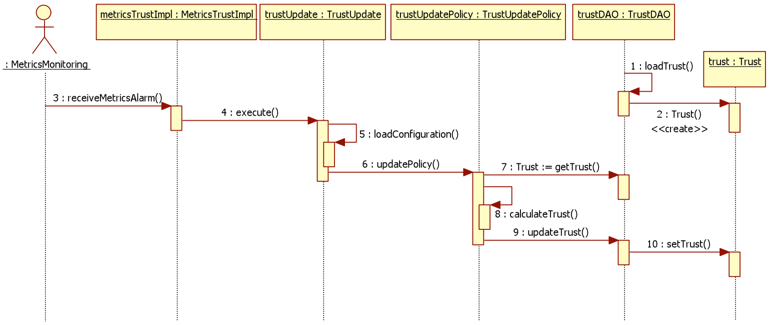


Fig. 6. Trust Management Architecture: Sequence Diagram

Specifically, when a member in SR x interacts with a another specific SR member in the same SR its reputation is computed using the following function:

$$f_x = \frac{\sum_{i=1}^{n} R_i \cdot T_{i,x} + R_x}{n+1} \tag{3}$$

where R_i represents the reputation value provided by SR i, $T_{i,x}$ is the reputation of SR i with respect to SR members in SR x, R_x is the current reputation of the specific member with respect to the other members and, finally, n is the number of reputation values read from other SRs.

The value returned by the function is the new reputation computed after each interaction with the member. Note that, since we assume interactions to be deterministic (e.g. we assume that all interactions with the member happens with the same order for all the other members in an SR) and the method used to calculate f is deterministic, all members in SR x agree on the reputation value toward the specific SR member.

After some interactions we suppose that administrators at each member can check through a set of facts the exact behaviour of a specific SR member. This can be modelled by defining the function g. In our case, g is defined in such a way that the current reputation value for a member is modified after each verification and increased if the verification confirms the expectations ($R_x \geq 0.5$ and correct behaviour or $R_x < 0.5$ and bad behaviour), and reduced otherwise. The same type of update is executed on the reputation values for other SRs too: if the reputation value read from an SR confirms the verified behaviour of the specific SR member, the corresponding reputation value is increased, otherwise it is decreased. More specifically we used the following function:

$$g = (-1)^s \cdot K \cdot \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-0.5)^2}{2\sigma^2}} \tag{4}$$

where K is a constant real multiplicative factor, σ is the standard deviation and s is parameter that has value 0 if the verification confirms the reputation value or value 1 otherwise (we assumed $K = 0.005$ and $\sigma = 0.15$). The rationale behind this formula is that reputation values in the middle of the range are not useful to take decisions; therefore, the formula is designed to quickly polarize the reputation value either towards a large or small value and then maintain the reputation in this state despite possible sources of fluctuations.

Using these functions we have also conducted an experimental evaluation in order to assess the effectiveness of our approach. For the sake of brevity, we do not include these results in this paper; interested readers can refer to [21] for detailed results.

5 Conclusions

In this paper, we have introduced the SR abstraction that allows financial institutions to share and process high volumes of events concerning massive threats (e.g., stealthy scans, Distributed Denial of Service) in a private and secure way. This collaborative event processing facilitates the correlation of suspicious events that would otherwise be overlooked by isolated institutions. The identification and prediction of those threats can thus trigger timely local reactions. Such sharing of sensitive information raises trust issues with respect to the information flowing in the SR. Robust mechanisms that ensure a measurable level of trust among distrusting SR participants are therefore required. To this end, we have proposed a Trust Management architecture that monitors, stores, and updates trust levels of SR members based on the behaviours of those members. In doing so, it interacts with both the Event Processing subsystem, in order to evaluate the events generated by the members, and the MeMo subsystem, in order to dynamically update the level of trust. Monitoring of SR contract rights and obligations allows members adherence to SR contract requirements (including trust thresholds) to be evaluated and incorporated into the trust feedback loop. The TM design is highly flexible and allows for different trust update policies. In this paper, we have described the design and a preliminary implementation of a policy that computes and manages at run time the reputation of SR members based on their behaviours in the SRs and their reputation in other SRs that they may belong to.

Both the design and implementation of our TM and the other subsystems are still preliminary: we are currently working in the context of the EU funded project CoMiFin in order to enhance and extend them and evaluate them in more complex scenarios (e.g., asynchronous settings and failures in the collaborative SR environment).

Acknowledgements

This research is partially funded by the EU project CoMiFin (Communication Middleware for Monitoring Financial Critical Infrastructure). The authors wish to thank their project colleagues for their comments on the described design and implementation.

References

1. Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., Weaver, N.: Inside the Slammer Worm. IEEE Security and Privacy 1, 33–39 (2003)
2. DDoS: National Australia Bank it by DDoS attack. `http://www.zdnet.com.au/news/security/soa/National-Australia-Bank-hit-by-DDoS-attack/0,130061744,339271790,00.htm` (2010)
3. DDoS: Update: Credit card firm hit by DDoS attack, `http://www.computerworld.com/securitytopics/security/story/0,10801,96099,00.html` (2010)
4. Fraud: FBI investigates 9 Million ATM scam (2009), `http://www.myfoxny.com/dpp/news/090202_FBI_Investigates_9_Million_ATM_Scam`
5. Locasto, M.E., Parekh, J.J., Keromytis, A.D., Stolfo, S.J.: Towards collaborative security and p2p intrusion detection. In: IEEE Workshop on Information Assurance and Security. United States Military Academy, West Point (2005)
6. Staniford, S., Hoagland, J.A., McAlerney, J.M.: Practical automated detection of stealthy portscans. Journal of Computer Security 10, 105–136 (2002)
7. Zhou, C.V., Leckie, C., Karunasekera, S.: A survey of coordinated attacks and collaborative intrusion detection. Computer and Security 29, 124–140 (2010)
8. CoMiFin: CoMiFin - Communication Middleware for Monitoring Financial Critical Infrastructures (2010), `http://www.comifin.eu`
9. Krügel, C., Toth, T., Kerer, C.: Decentralized event correlation for intrusion detection. In: Kim, K.-c. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 114–131. Springer, Heidelberg (2002)
10. Xie, Y., Sekar, V., Reiter, M.K., Zhang, H.: Forensic analysis for epidemic attacks in federated networks. In: ICNP, pp. 43–53 (2006)

11. Cachin, C., Keidar, I., Shraer, A.: Trusting the cloud. SIGACT News 40, 81–86 (2009)
12. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: Above the clouds: A berkeley view of cloud computing. Technical report, University of California, Berkeley (2009)
13. Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In: WWW 2003: Proceedings of the 12th international conference on World Wide Web, pp. 640–651. ACM, New York (2003)
14. Sun, L., Jiao, L., Wang, Y., Cheng, S., Wang, W.: An adaptive group-based reputation system in peer-to-peer networks. In: Deng, X., Ye, Y. (eds.) WINE 2005. LNCS, vol. 3828, pp. 651–659. Springer, Heidelberg (2005)
15. Huynh, T.D., Jennings, N.R., Shadbolt, N.R.: An integrated trust and reputation model for open multi-agent systems. Autonomous Agents and Multi-Agent Systems 13, 119–154 (2006)
16. Gupta, M., Judge, P., Ammar, M.: A reputation system for peer-to-peer networks. In: NOSSDAV 2003: Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video, pp. 144–152. ACM, New York (2003)
17. Zhu, Y., Shen, H.: Trustcode: P2p reputation-based trust management using network coding. In: Sadayappan, P., Parashar, M., Badrinath, R., Prasanna, V.K. (eds.) HiPC 2008. LNCS, vol. 5374, pp. 378–389. Springer, Heidelberg (2008)
18. Bachrach, Y., Parnes, A., Procaccia, A.D., Rosenschein, J.S.: Gossip-based aggregation of trust in decentralized reputation systems. Autonomous Agents and Multi-Agent Systems 19, 153–172 (2009)
19. Nagios: Nagios (2010), `http://www.nagios.org`
20. Tivoli: IBM Tivoli Monitoring (2010), `http://www-01.ibm.com/software/tivoli/products/monitor/`
21. Baldoni, R., Doria, L., Lodi, G., Querzoni, L.: Managing reputation in contract-based distributed systems. In: OTM Conferences (1), pp. 760–772 (2009)

Using MPLS in a Wireless Mesh Network to Improve the Resiliency of SCADA Systems

Stefano Avallone[1,2] and Salvatore D'Antonio[3,2]

[1] University of Naples "Federico II", Via Claudio 21, 80125 Naples, Italy
`stefano.avallone@unina.it`
[2] CINI Consorzio Nazionale Interuniversitario per l'Informatica, Italy
[3] University of Naples "Parthenope", Centro Direzionale di Napoli, Isola C4, 80143 Naples, Italy
`salvatore.dantonio@uniparthenope.it`

Abstract. Critical infrastructure are often and often being managed by SCADA systems that communicates using the *de facto* standard TCP/IP suite of protocols. Given the recent advances in wireless communications and the cost-effectiveness of deploying a multi-hop wireless network, we also foresee the use of wireless networks as the communication infrastructure of SCADA systems in the near future. In order for that to happen, the needed requirements of SCADA systems in terms of performance, reliability and resiliency must be ensured. To this end, a critical role is played by the routing protocol. In a previous work, we proposed a forwarding paradigm for wireless networks which was shown to be robust against node/link failures. However, such a forwarding paradigm cannot be used as-is in the case of SCADA systems due to its loose control over the network traffic. In this paper, we present an alternative implementation of such forwarding paradigm, which uses MPLS – a widely adopted technology in the wired world – as its forwarding engine and describe how such solution solves the issues presented by the original version of our forwarding paradigm.

Keywords: SCADA systems, network resiliency, MPLS, wireless mesh networks.

1 Introduction

Critical infrastructures are usually managed with the aid of SCADA (Supervisory Control And Data Acquisition) systems, which consist of several RTUs (Remote Terminal Units) sensing physical parameters and servers where human operators can have a picture of the real-time situation. RTUs are typically sensors that monitor physical parameters of interest and transmit the sensed data to the SCADA servers. It is therefore clear that the communication between RTUs and servers plays a fundamental role in the ability to keep the system under control and promptly react to failures. It is indeed needed a fast, secure and reliable communication between RTUs and SCADA servers. Historically, such communication has been ruled by proprietary solutions. More recently, however, the

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 440–450, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

widespread adoption of the TCP/IP suite of protocols has pushed a big technological change in the communication infrastructure of SCADA networks. In the last years, indeed, a growing number of SCADA systems are being realized (or converted to) using the standard TCP/IP suite of protocols. Such a move brings many advantages, such as for instance a large base of well established protocols. They are well known protocols, which makes it easier to design, maintain and troubleshoot the communication infrastructure. Also, it is easier to interconnect different sites through the public Internet.

There is, however, the other side of the coin. The use of well known protocols and the interconnection with the public Internet expose the SCADA systems to malicious attacks. It is thus of utmost importance to guarantee the secure operation of SCADA systems while exploiting the advantages of the use of standard protocols. Also, the TCP/IP suite of protocols has been designed for a computer network offering data delivery in a best effort manner, while SCADA systems have precise requirements in terms of reliability and timeliness of the delivery of messages. As a consequence, it is necessary to employ all the instruments that have been designed in the TCP/IP world to meet such requirements.

In this paper, we focus on the routing layer of the communication infrastructure, which can play a key role in achieving the goal of having the TCP/IP suite of protocols meet the requirements of SCADA systems. Indeed, routing determines the path taken by packets and hence it may allow to:

- find a proper path that ensures timeliness in the delivery of messages
- re-route packets around a failed node/link
- re-route packets around an attacked node

Thus, routing can help make a SCADA system resilient to both failures and attacks, while at the same time achieving their communication requirements.

Moreover, the communication between RTUs and SCADA servers has typically made use of a cabled infrastructure. With the growing spread and continuos enhancements of wireless communications, we also foresee the use of a wireless infrastructure to transport messages between RTUs and SCADA servers. A wireless network has many advantages over the cabled counterpart, such as low cost and easiness of deployment and maintenance due to lack of cables and speed of repairing (think of cables inadvertently cut by humans or by animals). Given the emergence of multi-hop techniques, it is nowadays possible to cover large areas using wireless technologies. Wireless networks where nodes are not mobile and form a backbone that routes packets generated by possibly mobile clients are denoted as wireless mesh networks [1]. In fact, there are more and more cases of city-wide wireless mesh networks witnessing the potential of such technology. Thus, we envisage the possible use of wireless mesh networks as wireless communication infrastructures for SCADA systems.

The main challenge when dealing with wireless networks is that interference exists between simultaneous transmissions taking place on the same frequency channel and in the same neighborhood. Thus, the routing algorithm should also take interference into account while pursuing the above mentioned objectives. In [2], we proposed a Layer-2.5 forwarding protocol with the goal of achieving high throughput and providing fast reaction to node/link failures, though the focus was not on SCADA systems. In this paper, we design an enhancement of the Layer-2.5 forwarding protocol to overcome some issues pointed out in [2] and increase its robustness, in order for it to address the hard requirements of SCADA systems. In particular, we show how MPLS (Multi-Protocol Label Switching) [3], a forwarding mechanism designed for and widely adopted in wired networks, can be effectively used to enhance the performance of our routing protocol for wireless mesh networks.

The rest of the paper is structured as follows. Section 2 briefly introduces how MPLS works, while Section 3 gives an overview of the characteristics of wireless mesh networks. Section 4 presents some details of the previously proposed Layer-2.5 forwarding paradigm and analyzes some of its issues. Section 5 describes the proposed implementation of the Layer-2.5 forwarding paradigm by using MPLS as its forwarding engine. Finally, Section 6 concludes this paper.

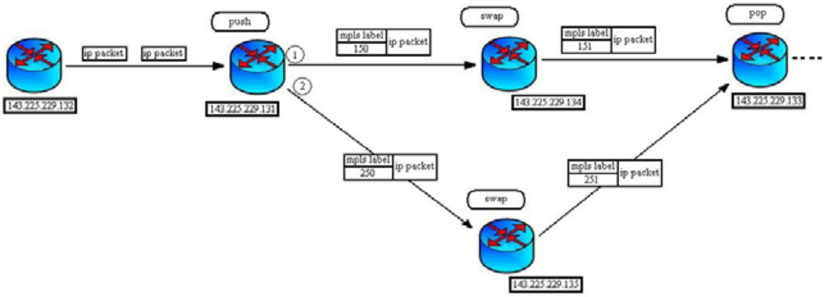
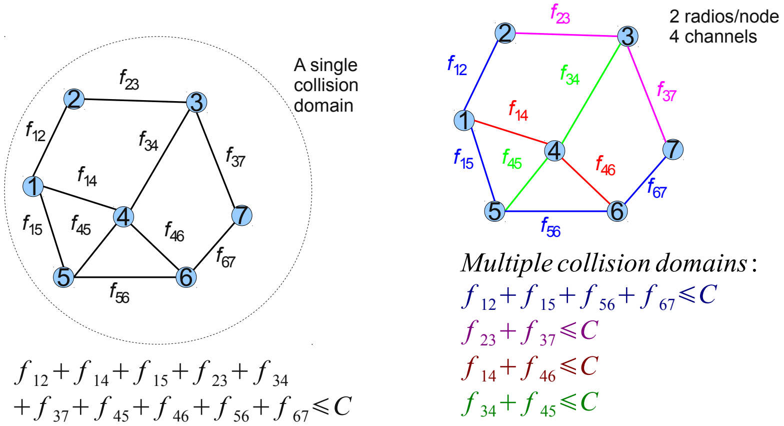


Fig. 1. Label switching in an MPLS network

2 Multi-Protocol Label Switching

MPLS is a forwarding paradigm that sits between the IP layer (or other layer-3 protocols) and a data link technology, hence it is often referred to as a layer-2.5 protocol. MPLS makes use of virtual circuits, that are denoted as Label Switched Paths (LSPs) in the MPLS jargon, and the forwarding is based on the switching of labels at every hop (fig. 1). For this purpose, a shim header is inserted between the layer-3 header and the layer-2 header which includes a 20-bit label that determines the next hop and the new label to be inserted into the packet. Clearly, it follows that, in an MPLS network, a packet is always processed by the MPLS entities and it is never passed to the IP entities, but when exiting the MPLS network. Thus, the path taken by packets is determined by how the MPLS forwarding tables have been configured. With respect to the IP routing, the MPLS forwarding enables two important features that give MPLS a great flexibility. First, packets are not constrained to follow the least cost path to the destination, but can follow any path, provided that labels have been properly configured. Second, while in the IP routing a Forwarding Equivalence Class (FEC), i.e., the set of all the packets that are routed in the same manner, is represented by all the packets destined to the same node, in the MPLS forwarding a FEC can be identified by different criteria including source node, source and destination ports and a combination of them. Thus, in an MPLS network, it is possible that packets destined to the same node but having, e.g., different destination ports are routed along distinct paths.

Another important feature of MPLS is that it allows fast mechanisms to recover from a node/link failure (possibly due to an attack). When a failure occurs in an IP network, it is necessary to wait for a node to detect the failure and then for the convergence time, i.e., the time necessary for nodes to exchange routing messages and have all a consistent view of the network topology. With MPLS, instead, it is possible to pre-configure alternative paths, denoted as backup paths, that can be used in case of failure of the active paths. The down-time is thus restricted to the time necessary for a node to detect the failure. There are several possible mechanisms for MPLS restoration. For instance, the backup path may be path disjoint or single node/link disjoint with respect to the active path. In the former case, the active path and the backup path do not share any link or node. In the latter case, different backup paths are pre-established, each of which protects against a failure of a single link or a single node.


A single collision domain
f_{12}
f_{23}
f_{34}
f_{37}
f_{14}
f_{15}
f_{45}
f_{46}
f_{56}
f_{67}
1
2
3
4
5
6
7
$f_{12}+f_{14}+f_{15}+f_{23}+f_{34}+f_{37}+f_{45}+f_{46}+f_{56}+f_{67}\leqslant C$
2 radios/node
4 channels
Multiple collision domains:
$f_{12}+f_{15}+f_{56}+f_{67}\leqslant C$
$f_{23}+f_{37}\leqslant C$
$f_{14}+f_{46}\leqslant C$
$f_{34}+f_{45}\leqslant C$

(a) Single-radio case

(b) Multi-radio case

Fig. 2. Constraints on the available bandwidth

3 Wireless Mesh Networks

Wireless mesh networks have emerged as an infrastructure to create wireless backbones that extend the coverage of traditional WLANs by routing packets from one mesh router to another through multiple wireless hops. As wireless transmissions are involved, interference is to be taken into account. The main effect of interference is to prevent simultaneous transmissions to take place on the same frequency channel, which implies that a node cannot use the whole capacity of the wireless link, but all the nodes in a neighborhood have to share the channel capacity. Thus, the main difference between the wired scenario and the wireless scenario is that in the latter one the bandwidth available on a link is less than the link capacity. This situation is illustrated in Fig. 2a, where we assume that all the links belong to the same collision domain and denote by f_{ij} the bandwidth available on link $i \rightarrow j$. If all the nodes have a single radio and therefore transmit on the same frequency channel, then the channel capacity must be shared among all the links, and hence the sum of the available bandwidth on all the links must not exceed the channel capacity C.

Given the recent availability of cost-effective wireless network interface cards, multi-radio devices have been introduced [4,5] in order to increase the throughput of a wireless mesh network. Indeed, wireless standards provide multiple orthogonal channels (e.g., the IEEE 802.11b/g and IEEE 802.11a standards define, respectively, 3 and 12 non-overlapping channels) and mesh nodes can exploit the availability of multiple radios to transmit/receive simultaneously on non-interfering channels. Figure 2b shows the improvement in performance brought by multiple radios. If different links in a neighborhood transmit on distinct channels, the result is a splitting in multiple collision domains, each associated with a channel. In each collision domain the constraint that the sum of the bandwidth available on the links must not exceed the channel capacity still holds. However, as fig. 2b shows, collision domains are now smaller with respect to the single-radio case, which allows for higher link bandwidth availability and hence higher network throughput.

Figure 2 clearly shows that the amount of bandwidth available on each link depends on how channels are assigned to links, which determines the formation of collision domains. Since routing should be tailored to the bandwidth available on links, it turns out that channel assignment and routing are strictly inter-dependent on each other. In fact, a conspicuous amount of papers [6,7,8,2,9,10] have been published addressing the joint channel assignment and routing problem. In particular, in [2] we proposed a joint channel assignment and routing algorithm which computes a channel assignment and the resulting available bandwidth on each link, Also, we proposed a forwarding paradigm, denoted as Layer-2.5 forwarding paradigm, to route packets in order to utilize network links according to the computed bandwidth availablility. Such forwarding paradigm is illustrated in some details in the next section.

4 A Layer-2.5 Forwarding Paradigm

In this section, we provide some details on the Layer-2.5 forwarding paradigm (L2.5) we proposed in [2]. We refer to [2] for more details. L2.5 requires that a solution to the joint channel assignment and routing problem has been found and thus each radio is assigned a channel and each wireless link is associated with a flow rate value. The goal is to enable every router to utilize each of its links in proportion to their flow rates. We underline that the operations of our forwarding paradigm do not involve the use of destination-based routing tables.

Each router is not required to have a complete knowledge of the network topology, but only the information about the minimum hop count to each possible destination in the WMN. We denote by $\boldsymbol{HC}_u$ the *hop count* vector of node u, whose component $HC_u(d)$ represents the hop count from u to the destination d. A simple procedure for having the routers build their own hop count vectors is described in [2]. Such hop count vectors, however, are not directly used to forward packets along the shortest paths. Instead, each router u sets a timer which expires at regular intervals and records the amount of bytes $b(v)$ sent to each neighbor v since the last timer expiration. Every time u has to take a forwarding decision, it computes the gap $\Delta_u(v)$ between the desired and the current utilization of link $u \rightarrow v$ for each neighbor v:

$$\Delta_u(v) = \frac{f(u \rightarrow v)}{\sum_{\forall u \rightarrow i} f(u \rightarrow i)} - \frac{b(v)}{\sum_{\forall u \rightarrow i} b(i)}$$

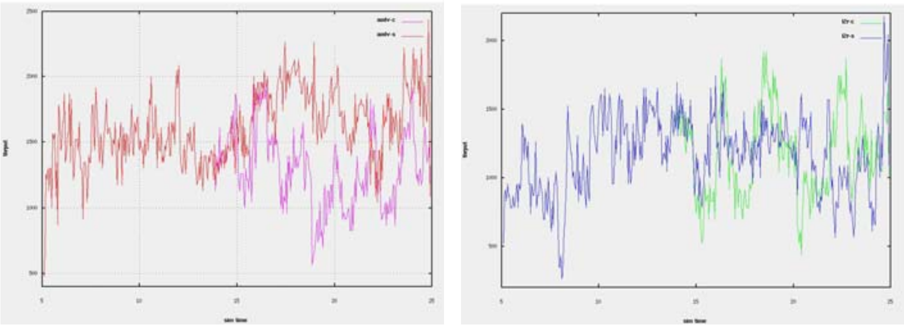
In the attempt to keep the transmission rate on all of its links proportional to the corresponding flow rate, router u will send the packet to the neighbor node having the largest $\Delta_u(v)$ value. Clearly, a router cannot decide the next hop of a packet based only on the $\Delta_u(v)$ values, as packets could take extremely long paths to get to destination. This is where the hop count vectors come into play. In the process of building its own hop count vector, each router also learns the hop count of its neighbors to every destination. This information is used to partition the neighbors based on the hop count to a certain destination. For a generic destination d, the set $\mathfrak{N}(u)$ of neighbors of node u is partitioned into three sets: $\mathfrak{N}_d^{=}(u)$ (containing the neighbors with the same hop count to d as u), $\mathfrak{N}_d^{+}(u)$ (containing the neighbors with u's hop count to d plus 1) and $\mathfrak{N}_d^{-}(u)$ (containing the neighbors with u's hop count to d minus 1).

L2.5 provides that every source node s in the WMN puts a *maximum hop count* value into the HC^{max} field of the *L2.5 header* of each packet it sends. Such a value equals the minimum hop count to the destination multiplied by a constant factor $\alpha > 1$. The value into the HC^{max} field is decremented at each intermediate hop and is used to determine the set of candidate next hop neighbors for a packet. Indeed, each intermediate router must take a forwarding decision that allows the packet to reach the destination within HC^{max} hops. Thus, for instance, if the value in the HC^{max} field equals the minimum hop count to the destination for the intermediate node u, then the packet must be necessarily sent to a neighbor in $\mathfrak{N}_d^{-}(u)$ and will thus follow a minimum hop path. Otherwise, the packet may also be sent to neighbors in $\mathfrak{N}_d^{=}(u)$ or even $\mathfrak{N}_d^{+}(u)$. The neighbor v with the maximum $\Delta_u(v)$ among those in the set of candidate next hop neighbors is then selected.

More precisely, a router u receiving a packet from node w with maximum hop count HC_u^{max} and destined to node d, determines the set $\mathfrak{S}$ of candidate next hop neighbors as follows:

$$\mathfrak{S} = \begin{cases} \mathfrak{N}(u) - \{w\} & \text{if } HC_u^{max} > HC_u(d) + 1, \\ \mathfrak{N}_d^{=}(u) \cup \mathfrak{N}_d^{-}(u) - \{w\} & \text{if } HC_u^{max} = HC_u(d) + 1, \\ \mathfrak{N}_d^{-}(u) - \{w\} & \text{if } HC_u^{max} = HC_u(d). \end{cases} \tag{1}$$

According to L2.5, thus, a router u determines the set $\mathfrak{S}$ of candidate neighbors, computes $\Delta_u(v)$ for all neighbors $v \in \mathfrak{S}$, decrements the HC^{max} field and sends the packet to the neighbor $v \in \mathfrak{S}$ with the maximum $\Delta_u(v)$.



(a) AODV (b) L2.5

Fig. 3. Instantaneous throughput with (-c) and without (-s) a node failure

4.1 Analysis of L2.5

The proposed Layer-2.5 forwarding paradigm aims at taking the link bandwidth availability resulting from a channel assignment into account in order to increase the network throughput. Also, L2.5 does not use routing tables in order to rapidly react to node/link failures. Indeed, if an intermediate node fails, L2.5 can rapidly avoid sending packets to the failed node by simply eliminating it from the set of candidate next-hop nodes. Recovering from a failure also does not require to exchange information among nodes, thus avoiding to generate overhead traffic. We compared L2.5 to AODV [11] (a destination-based routing protocol which uses routing tables) by evaluating their reaction to node failures. For this purpose, we conducted some simulations by using the *ns-2* network simulator. Figure 3 shows the results of one of such simulations. At a given time instant (time instant 14 in the simulation), a node failure is simulated. Figures 3a and 3b show the instantaneous throughput during the simulation time with and without the node failure achieved by AODV and L2.5, respectively. We can observe that, with respect to the case with no failure, the throughput decrease for AODV is of 0.3 Mb/s after 1 second from the failure and more than 1 Mb/s after 4 seconds. Thus, a destination-based routing protocol such as AODV takes a significant amount of time to recover from the node failure. L2.5 instead shows a decrease of 0.3 Mb/s in the throughput after 2 seconds but soon after recovers the average throughput achieved in the failure-free scenario.

However, the mechanism used by L2.5 to keep the utilization of network links close to their flow rate turns to be also one of its limits. Indeed, despite L2.5 ensures that packets reach the destination in at most *maximum hop count* hops (which is usually α times the length of the shortest path, as determined by the source mesh router), it cannot avoid that packets take long path to the destination. Simulations have shown that most of the packets take exactly *maximum hop count* hops to the destination. Despite a countermeasure has been proposed in [2] (the introduction of a parameter *beta* which weighs $\Delta_u(v)$ depending on the ratio of the minimum hop count to the destination to the residual *maximum hop count*), such issue is not solved, but simply converted into a trade-off between accurate link utilization and limited path length. The basic problem is that L2.5 does not provide adequate control over the paths taken by packets and the underlying IP layer does not allow to differentiate among packets belonging to different flows. In the next section we show how the use of MPLS allows to better implement the idea behind L2.5 and thus avoid the drawbacks described so far.

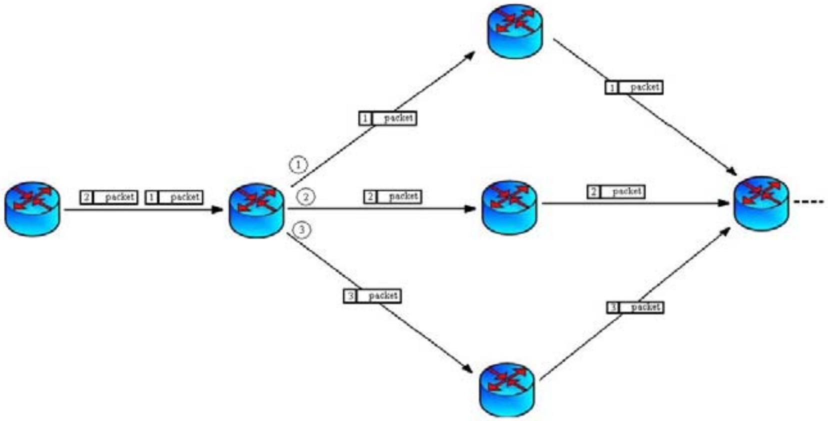


Fig. 4. Splitting in an MPLS network

5 Implementing L2.5 in an MPLS Network

Based on the above description of L2.5, it should be clear that MPLS cannot be used as is to support L2.5. Indeed, with L2.5 each node forwards packets to its neighbors based on the utilization of its links, regardless of the flow they belong to. Consequently, the packets of a flow follow multiple distinct paths. MPLS, instead, establishes tunnels and maps each flow onto a single tunnel. Hence, all the packets of a flow are routed along the corresponding tunnel. Thus, we would need the ability to split MPLS packets across multiple tunnels. Fortunately, we have already implemented a non-standard feature [12] (as a patch against the Linux kernel) that allows an MPLS router (there is a project [13] adding MPLS support to the Linux kernel) to split the packets of a flow across multiple tunnels (fig. 4). Different policies can be used at a node to select one of the multiple outgoing tunnels. The simplest one is clearly the round robin strategy, but advanced policies which take the current link load into account can be implemented. If all the network nodes are given such a splitting capability, then MPLS can be effectively used to support L2.5.

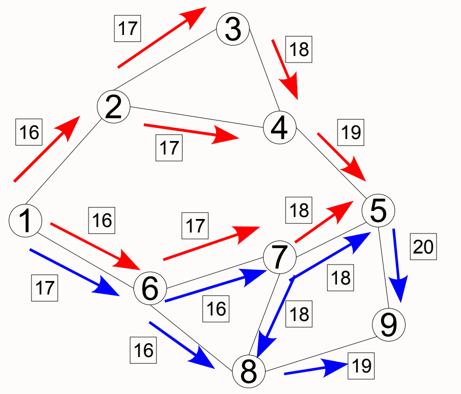


Fig. 5. Splitting in a wireless mesh network

Figure 5 shows how it is possible to implement L2.5 by using MPLS enhanced with the splitting feature. In particular, MPLS labels can be configured to force a given flow to follow a pre-determined set of paths. For instance, node 1 in fig. 5 can be configured so that it splits the packets destined to node 5 between node 2 and node 6 (red arrows). In both cases, the label pushed into those packets is 16. If labels are configured properly, the packets of the flow between nodes 1 and 5 follow all the possible paths marked with red arrows (there are actually three possible such paths). At node 1, instead, packets destined to node 9 are all sent to node 6 using label 17. Node 6 can know which flow each received packet belongs to by simply inspecting its MPLS label: packets of the flow 1→5 are labelled with 16, while those of the flow 1→9 are labelled with 17. Packets of the former flow are all sent to node 7, while packets of the latter flow are split between node 7 and 8. Thus, node 6 can differentiate the forwarding of packets based on the flow they belong to. This capability is simply not possible with plain IP and allows a strict control over the path taken by packets.

The use of MPLS to implement L2.5 brings several important advantages:

- MPLS is a standard, well known forwarding paradigm with a large base of installations
- MPLS provides strict control over the path followed by packets. It is thus possible to avoid that packets take long paths
- By using distinct labels for different flows, it is possible to differentiate the forwarding of packets belonging to different flows
- The MPLS header includes a TTL field, whose value can be used at an intermediate node to determine how many hops a packet has already travelled

The main drawback of L2.5 is the scarce control over the path taken by packets, which is solved by using MPLS. MPLS is thus a powerful instrument which gives us high flexibility in the management of the traffic crossing the network. Also, MPLS enables us to use standard mechanisms to provide some functionalities (e.g., the standard TTL field in the MPLS header can be used as a counter of the hops taken by a packet). Clearly, in order to implement L2.5 by using MPLS in an efficient manner, it is needed:

- to properly engineer the possible paths taken by the packets of the flows between each source-destination pair
- to define a proper splitting policy, to be used at every node in order to keep the utilization of links close to the computed flow rates

In particular, a proper splitting policy should inspect the TTL field in the MPLS header of the received packet to determine the subset of outgoing tunnels that allow the packet to reach the destination in a *reasonable* number of hops. We assume that each node knows the maximum number of hops to reach the destination associated with each of the outgoing tunnels. Then, the outgoing tunnel can be selected by considering the link with the highest gap between the current utilization and the computed flow rate.

6 Conclusions and Future Work

Given the recent advances in wireless communications and the cost-effectiveness of deploying a multi-hop wireless network, we foresee the use of wireless mesh networks as the communication infrastructure of SCADA systems. A key role to provide the needed requirements in terms of performance, reliability and resiliency of SCADA systems is played by the routing protocol. In a previous work, we defined a forwarding paradigm for wireless mesh networks which was shown to be robust against node/link failures. However, such a forwarding paradigm cannot be used as-is in the case of SCADA systems due to its loose control over the network traffic. In this paper, we have proposed to use MPLS as the forwarding engine of our paradigm and described the resulting advantages. As future work, we plan to design efficient algorithm to compute the tunnels to be configured in the MPLS network and an efficient policy for the splitting mechanism.

Acknowledgments

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement No. 225553 (INSPIRE Project).

References

1. Akyildiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: a survey. Computer Networks 47(4), 445–487 (2005)
2. Avallone, S., Akyildiz, I.F., Ventre, G.: A Channel and Rate Assignment Algorithm and a Layer-2.5 Forwarding Paradigm for Multi-Radio Wireless Mesh Networks. IEEE/ACM Transactions on Networking 17(1), 267–280 (2009)
3. Rosen, E., Viswanathan, A., Callon, R.: Multiprotocol Label Switching Architecture. RFC 3031, IETF (January 2001)

4. Bel Air Networks, http://www.belairnetworks.com/products/
5. Proxim Wireless, http://www.proxim.com/
6. Raniwala, A., Gopalan, K., Chiueh, T.: Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks. ACM Mobile Computing and Communications Review 8(2), 50–65 (2004)
7. Alicherry, M., Bhatia, R., Li, E.: Joint Channel Assignment and Routing for Throughput Optimization in Multiradio Wireless Mesh Networks. IEEE Journal on Selected Areas in Communications 24(11), 1960–1971 (2006)
8. Kodialam, M., Nandagopal, T.: Characterizing the Capacity Region in Multi-Radio Multi-Channel Wireless Mesh Networks. In: Proc. of ACM MobiCom, pp. 73–87 (2005)
9. Mohsenian Rad, A.H., Wong, V.W.S.: Joint logical topology design, interface assignment, channel allocation, and routing for multi-channel wireless mesh networks. IEEE Transactions on Wireless Communications 6(12), 4432–4440 (2007)
10. Chen, Y.Y., Liu, S.C., Chen, C.: Channel assignment and routing for multi-channel wireless mesh networks using simulated annealing. In: Proc. of IEEE GLOBECOM, pp. 1–5 (November 2006)
11. Perkins, C., Belding-Royer, E., Das, S.: Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561, IETF (July 2003)
12. Avallone, S., Manetti, V., Mariano, M., Romano, S.P.: A splitting infrastructure for load balancing and security in an MPLS network. In: Proceedings of TridentCom 2007, Orlando, FL, USA. IEEE, Los Alamitos (May 2007)
13. MPLS for Linux, http://mpls-linux.sourceforge.net

Fusion of Bayesian and Ontology Approach Applied to Decision Support System for Critical Infrastructures Protection

Rafał Kozik[2], Michał Choraś[1,2], and Witold Hołubowicz[1,3]

[1] ITTI Ltd., Poznań
michal.choras@itti.com.pl
[2] Institute of Telecommunications, UT&LS Bydgoszcz
chorasm@utp.edu.pl
[3] Adam Mickiewicz University, Poznań
holubowicz@amu.edu.pl

Abstract. In this paper, a decision support system based on the ontology knowledge for Critical Infrastructure security assessment is presented. The ontology provides vulnerabilities, threats and safeguards classification and their relationships with other security aspects. Such knowledge is used to build Bayesian network, which is used to asses the severity level of the detected threats. Described approach is applied in decision support tool developed within the INSPIRE project aiming at increasing security and protection through infrastructure resilience. The major contribution of this paper is the fusion of the ontology and Bayesian approach utilized in the reasoning engine of the decision support application.

1 Introduction

Rapid success of information and communication systems had significant influence on developing new way of controlling and managing critical infrastructures. Systems monitoring and controlling critical infrastructures such as SCADA (Supervisory Control and Data Acquisition) moved from dedicated solutions for particular operator to integrated and IP-based frameworks.

However, such evolution exposed the system for cyber threats and cyber attacks and unauthorized access by hackers. This requires a new approach to critical infrastructure protection which will engage expert knowledge, decision support systems and such network elements as firewalls, intrusion and anomaly detection systems. Critical Infrastructure Protection (CIP) including cyber defense is one of the crucial security and safety aspects in EU [1].

Critical infrastructure security problems are the challenge for the EU FP7 ICT-SEC INSPIRE Project (INcreasing Security and Protection through Infrastructure REsilience). It is a two-year small or medium-scale focused research European project. More details about the project are available at: *http : //www.inspire − strep.eu.*

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 451–463, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

There are two main research directions in the project. The first one ("in-network") focuses on:

- analyzing and modeling dependencies between critical infrastructures and underlying communication networks,
- designing and implementing traffic engineering algorithms to provide SCADA (Supervisory Control and Data Acquisition) traffic with quantitative guarantees,
- exploiting Peer-to-Peer (P2P) overlay routing mechanisms for improving the resilience of SCADA systems,
- defining a self-reconfigurable architecture for SCADA systems,
- development of diagnosis and recovery techniques for SCADA systems.

The second research direction in the project, called "off-network" focuses on designing the INSPIRE Security Ontology and development of the decision support system to evaluate critical infrastructure security status. The role of the proposed DSS (called INSPIRE Decision Aid Tool - DAT) is to provide the SCADA operator system with all the necessary information about the threats and vulnerabilities the specific critical infrastructure is exposed to. Additionally, DAT can propose appropriate reactions and countermeasures for the particular threat.

The paper is structured as follows: in section 2 INSPIRE Decision Aid Tool (DAT) is motivated and presented. The underlying security ontology overview is given in section 2.3. Moreover, the ontology mapping mechanism and DAT knowledge organization are explained in sections 2.4 and 2.5, respectively. Then in section 3, our novel approach based on the fusion of the ontology knowledge and Bayesian network is presented in detail. Sample use case is presented and discussed in section 4. Conclusions are given afterwards.

2 INSPIRE Approach to Decision Support Systems

2.1 Overview of DSSs for Critical Infrastructures Protection

Decision Support Systems (DSS) are information systems that support human in different decision-making activities. DSS applications are successfully and widely used in industry and critical infrastructure protection (CIP). In 1987 Texas Instruments company released GADS (Gate Assignment Display System) decision support system for United Airlines. As a result, the travel delays have been reduced significantly. The system was used by the management of ground operations at various airports.

Another good example of successfully deployed decision support applications are expert systems in the banking area (expert systems for mortgages). The decision support systems are also widely used for river systems management to effectively cope with floods. For example, The German Federal Institute of Hydrology (BfG) funded the development of a Decision Support System for the Elbe river system. The great flooding in summer 2002 demonstrated the importance of such solutions.

Some examples of DSS used in the energy sector are described in [2]. DSS are also successfully deployed in nuclear power plants [3], urban water pollution control [4] or oilfield flood precaution [5].

2.2 INSPIRE DAT (Decision Aid Tool)

All the mentioned DSS examples are customized and focused on some particular branch of critical infrastructures. Decision Support Systems are usually designed for special kind of industry or application. Although they use different methodologies (Bayesian, multiagent, HMM), they rarely use ontologies description to support reasoning.

Therefore, in the INSPIRE project we proposed the security ontology, which mimics the complicated relationships between SCADA components and security aspects. Our ontology is a representation of relationships between particular classes (or instances) and as it is, cannot provide any knowledge-based reasoning or give feedback to its operator, therefore the INSPIRE Decision Aid Tool has been developed.

DAT is general and applicable to more than one critical infrastructure. It focuses on the SCADA properties to enhance protection and security of critical sectors. INSPIRE Decision Aid Tool may be also considered as a framework since it is reconfigurable by means of uploading other ontologies or various SCADA system topologies.

Two types of users (actors) are specified in DAT (Fig. 1):

- DAT User – user who wants to asses the systems security level.
- Expert – user who maintains security rules (facts about concerned system and relations between its elements), which allow to enrich the knowledge stored in ontology.

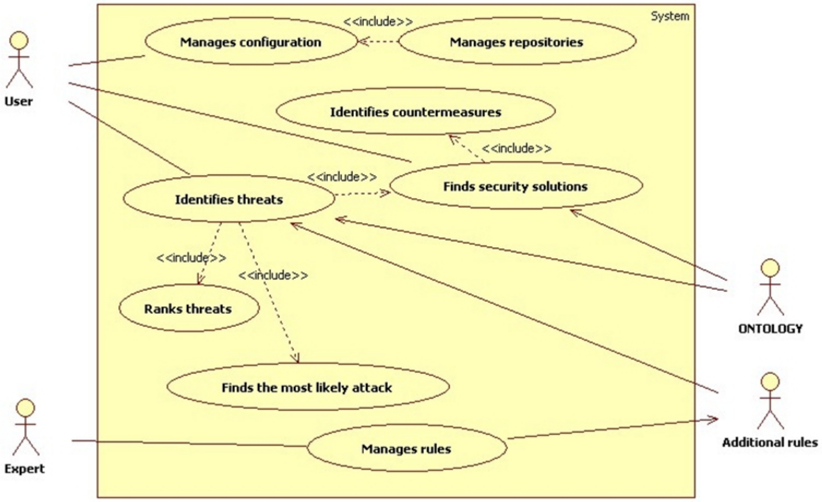


Fig. 1. DAT use cases

DAT is facilitated with user-friendly graphical interface which allows to identify and rank the threats found in critical infrastructures. Furthermore, the DAT allows user to find security solutions for particular threat and finds adequate countermeasures and strategy for minimizing the risk. What is more, DAT allows user to perform simulation scenario answering the questions such as "what may happen if particular action is taken" or "what happens (in terms of security) when particular equipment or software is added".

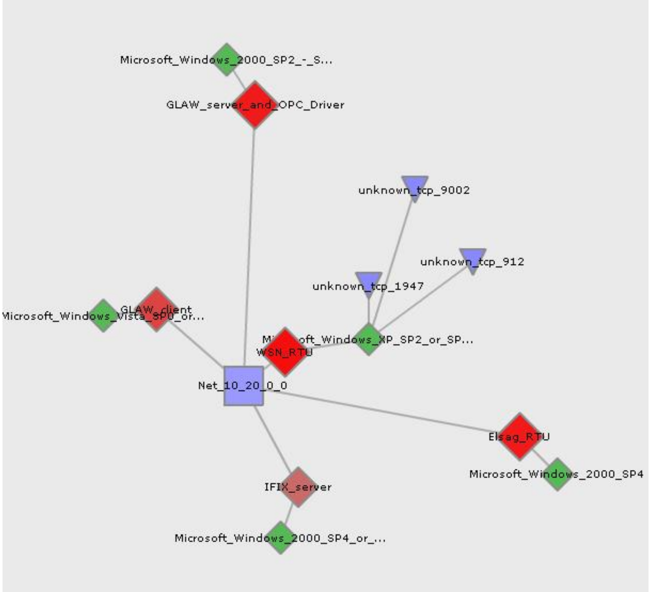

Microsoft_Windows_2000_SP2_-_S...
GLAW_server_and_OPC_Driver
unknown_tcp_9002
unknown_tcp_912
unknown_tcp_1947
Microsoft_Windows_Vista_SP0_or...
GLAW_client
Mi oft_Windows_XP_SP2_or_SP...
WSN_RTU
Net_10_20_0_0
Elsag_RTU
Microsoft_Windows_2000_SP4
IFIX_server
Microsoft_Windows_2000_SP4_or_...

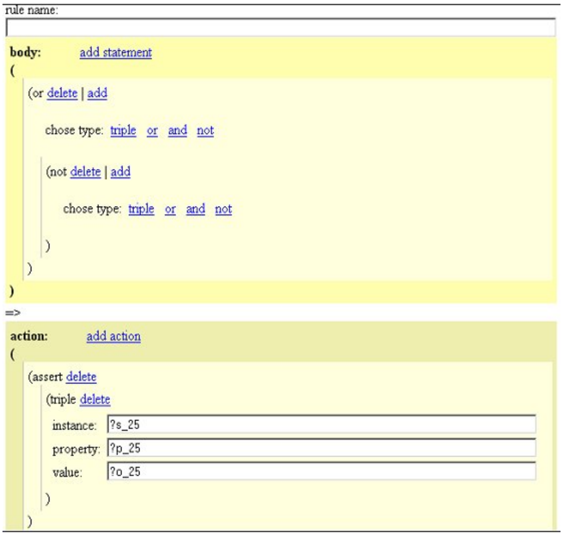
Fig. 2. Topology diagram and visualized threats (blinking red nodes)

The analysis performed by DAT is divided into three steps. Firstly, the topology diagram is rendered (Fig.2) to provide the operator with the information e.g. about CI elements interconnections, used applications etc. In the next step, the threats are visualized by the red blinking nodes (Fig. 2). Afterwards, the detailed security report is created to provide user with detailed information (Fig. 10). The used inference engine and ranking methodology remain transparent for the user. However, these can be configured and customized via the configuration panel.

Moreover, the mechanism for adding additional rules (expert security rules) has been created for experts and security operators. Such rules about security aspects can enrich the ontology knowledge and improve reasoning. The GUI for adding expert rules is presented in Fig. 3.

2.3 INSPIRE Security Ontology

Our approach to security ontology is based on ISO/IEC 133351:2004 standard [6]. According to the standard, vulnerabilities are considered as properties of a



instance: ?s_25
property: ?p_25
value: ?o_25

Fig. 3. GUI for expert rules generation

network security system. In such approach assets and components have weak points named vulnerabilities. These vulnerabilities can be exploited by threats, leading to attacks. This security system is depicted into a form of classification with properties and relationships between various security aspects [7][8].

2.4 Ontology Mapping

The proposed ontology is used by the Decision Aid Tool (DAT). However, the ontology format is not directly accepted by the inference engine and requires mapping.

Therefore instances (and also relation between instances) stored in ontology are mapped into facts and SWRL rules are mapped into production rules [9]. Afterwards the reasoning can be performed by the inference engine (in this case JESS inference engine has been adopted). DAT uses ontology classes and instances to acquire the knowledge as RDF triples and processes them in the rule engine [10]. Each RDF triple consists of:

- Subject,
- Predicate,
- Object.

Each triple is able to fully describe one property of the instance. The interpretation of a triple is that "subject" has property "predicate" whose value is "object". Such strategy allows DAT to be more flexible to ontology schema changes, because adding new properties to the particular instance has no impact on the mapping mechanism and no impact on DAT source code.

In example the relation "Asset x hasVulnerability y" is mapped into (triple (subject x) (predicate 'hasVulnerability') (object y)). The SWRL rules are mapped into production rules as follows:

$$hasParent(?x1, ?x2) \wedge hasBrother(?x2, ?x3) \Rightarrow hasUncle(?x1, ?x3)$$

is mapped into:

```
(defrule rule-1
(triple (predicate 'hasParent') (subject ?x1) (object ?x2) )
(triple (predicate 'hasBrother') (subject ?x2) (object ?x3) )
⇒
(assert (tiple (predicate 'hasUncle') (subject ?x1) (object ?x3) ) ). )
```

2.5 DAT - Knowledge Organization

The knowledge about the critical infrastructure maintained in the ontology is large and requires classification and additional organization in order to be efficiently used by the inferencing engine. The most reasonable solution is to organize it in a hierarchical manner (from low level facts to high level ones as in Fig.4).

Lowest layer (Fig. 4) of the knowledge stack simply represents the knowledge obtained from OWL thanks to mapping described in section 2.4. The RDF triples based description allows to extract information about basic relations between elements and particularly identify the root classes and instances belonging to that class (Asset, Vulnerability, Threat, Safeguard). These concepts allow to extract, so called "root facts" about critical infrastructure, thus such knowledge, describing relations "asset-vulnerability-threat", gives the user information, which is similar to this which can be found in typical vulnerability databases.

Therefore, we provided the second layer which additionally extracts the given critical infrastructure topology. Hereby, information about particular node, its connection to the network, running applications etc. can be found. This allows to identify additional facts about analyzed environment such as faults in elements connectivity, configuration faults, etc.

On top of this knowledge, DAT allows the user to provide security rules. Particularly, operator has ability to asses what may happen if particular action is taken.

Let us consider the scenario where the operator plans to take down the router during the maintenance of the CI network. DAT using the information about the connectivity and information about business importance about detached nodes (detached by shutting down the router) will alert that this may cause serious malfunction of CI (or alternatively, that it has no impact on it). Also operation of adding new machine to CI infrastructure may also be validated by DAT prior the physical manipulations, saving the time and eventually the money.

However, the knowledge described above seems condition-action based (if-then structure). Therefore, one more layer of knowledge in the stack is introduced to

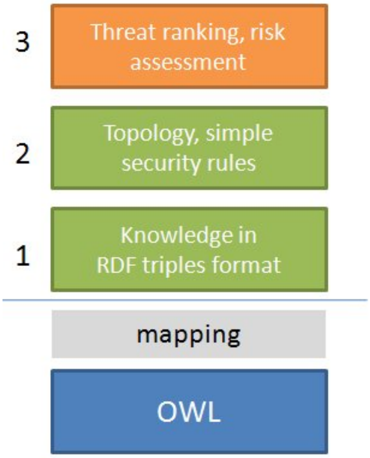

3
Threat ranking, risk assessment
2
Topology, simple security rules
1
Knowledge in RDF triples format
mapping
OWL

Fig. 4. DAT knowledge logical layers. Thanks to mapping the ontology (OWL file) is used to build two layers of DAT knowledge used to perform reasoning.

asses each threat (found in CI) severity level. It is done via the Bayesian network combined with the facts and rules maintained in bottom layers. More details follow in section 3.

3 Fusion of Bayesian Network and Ontology Knowledge

In this section the proposed approach to asses threats severity levels by means of Bayesian Network is presented. The general idea of fusion is presented in Fig. 5. The BN output computes the particular threat severity using observation about CI gained from ontology. The input is obtained from the first and the second layer of the knowledge stack. The first knowledge layer provides the network with the basic information about the threaten asset, threat itself, vulnerability and safeguard. The second layer, besides introducing the new threats using the security rules, allows to update the BN prior probabilities. For example added rules can increment the assets counters when new element is added to CI, or shape the particular node business value using some predefined conditions.

3.1 Structure of Proposed Bayesian Network

The structure of the proposed BN is presented in Fig. 6. The right arrows represent the input (observations), while the left arrows represent the posterior probability of fact the node is threaten by attack given the AT (Asset Type), VR (Vulnerability Risk) and SA (Safeguard Applied) observation.

Those observations are extracted by DAT using the knowledge about the CI. The AT observations represent the asset type. The information is adapted to emphasize the fact that some assets (elements in the CI) are more valuable than others.

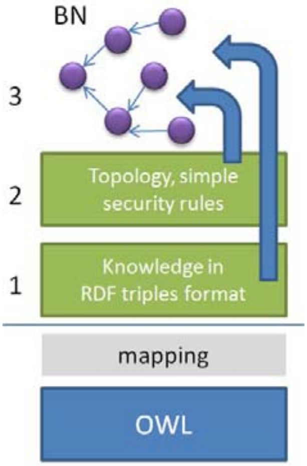

BN
3
2
Topology, simple security rules
1
Knowledge in RDF triples format
mapping
OWL

Fig. 5. Bayesian network is fed by the facts about CI from RDF triples, topology and simple security rules

Furthermore, the number of valuable assets also influences the total risk value. Particularly the AV (Asset Value) is used to increase the importance of SCADA servers, routers, RTUs and other critical elements. According to ISO standard [6], each network element may have vulnerabilities, which eventually put system in danger, therefore BN uses the VR (Vulnerability Risk) to evaluate its severity. The VR depends on the observation of fact that asset is applied and the VSL (Vulnerability Severity Level).

Eventually, the VR and AV are combined to asses the final value of the risk probability.

$$p(A=T|VRL,SA,AT)=\frac{p(A,VRL,SA,AT)}{p(VRL,SA,AT)} \tag{1}$$

3.2 Prior Probabilities Estimation Problem

The nominator in the equation 1 (based on the BN structure shown in Fig. 6) can be rewritten as in eq. 2:

$$\begin{aligned} p(A,VRL,SA,AT) = {} & p(VSL)p(AT)p(AS) \\ & p(AV|AT)p(VR|AS,VSL) \\ & p(A|VR,AV) \end{aligned} \tag{2}$$

In our approach, it is proposed to obtain probabilities distributions via the inferencing engine as is it shown in Fig. 5. Particularly the marginal probabilities distributions $(p(VSL),p(AT),p(AS))$ can be easily obtained via the histogram-based estimation method. In the example, the AT (asset type) variable can be

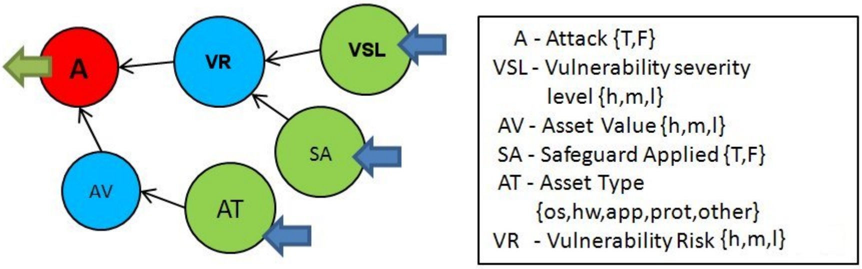

A
VR
VSL
SA
AV
AT
A - Attack {T,F}
VSL - Vulnerability severity level {h,m,l}
AV - Asset Value {h,m,l}
SA - Safeguard Applied {T,F}
AT - Asset Type {os,hw,app,prot,other}
VR - Vulnerability Risk {h,m,l}

Fig. 6. Bayesian network details (h=high, m=medium, l=low, t=true, f=false, os=operating system, app=application, prot=protocol, hw=hardware)

assigned one of the Asset classes names (particularly these classes in ontology which have instantiated individuals). The probability of particular AT is computed via single rule (JESS's engine production rule) which counts the number of instances belonging to particular class and divides this value by total number of all instances building the CI. The same approach is used for other marginal probabilities. The advantage is the fact when new elements are introduced (not only hardware but also software) these distributions are updated and eventually the estimated risk value is different.

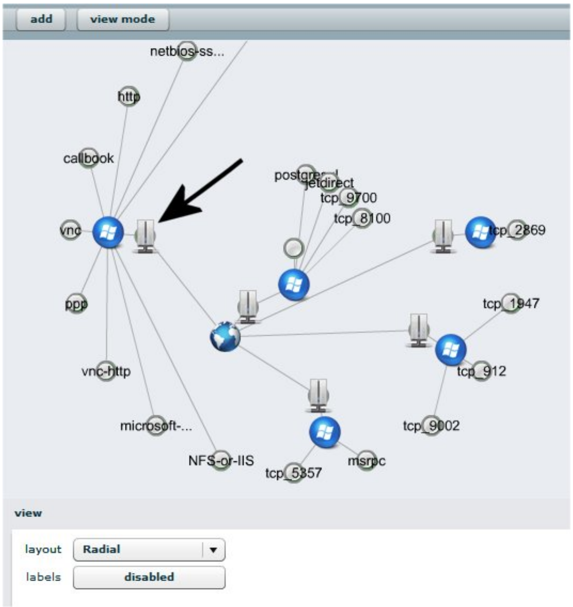
In our approach the conditional probabilities represent user defined preferences. Particularly $p(AV|AT)$ asses the given asset business value given the knowledge about its type, allows to stress the fact that some assets are more valuable than the others. In example user may define rule: "If AT is RTU then $P(AV = high|AT = RTU)$ is 0.99". The same approach is applied to $p(VR|AS, VSL)$ distribution.

The $p(A|VR, AV)$ (probability of attack given the VR an AV observation) is also strictly user depended (different users have different sense of balance between "asset business level" and "vulnerability risk"), and is computed using the same approach as for $p(AV|AT)$.

4 DAT Use Case Example

In this section the Decision Aid Tool demo is presented. The goal is to show "simulation mode" of the DAT, which allows to evaluate the risk of particular action prior to the physical manipulation. The demo uses ontology provided by "Topology Discovering Tool" and "Expert knowledge" provided by expert via DAT GUI interface and concerns following steps, where user:

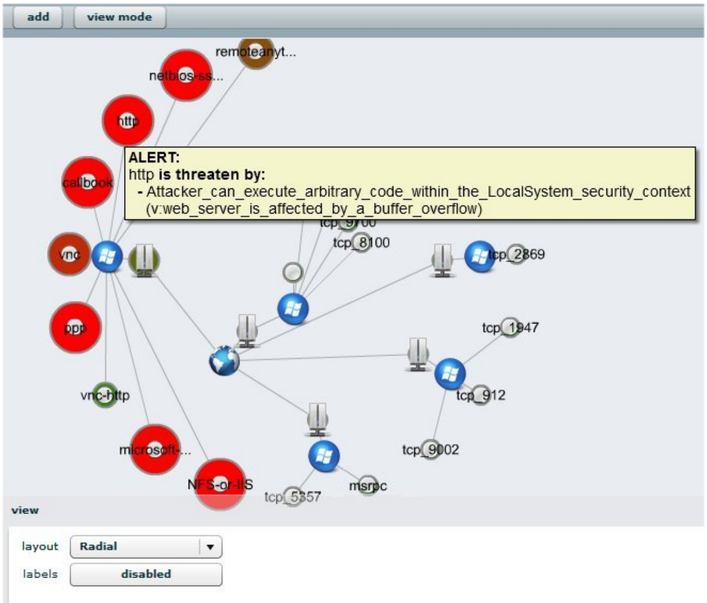
- uses DAT to visualize topology graph
- turns off firewall and ant-virus applications on one of the routers
- identifies the risks and visualizes topology again
- simulates installation of firewall and anti-virus application on affected OS



layout Radial

labels disabled

Fig. 7. Topology diagram (before security level assesment). The arrow indicates the router where the firewall and anti-viurs software will be switched off.

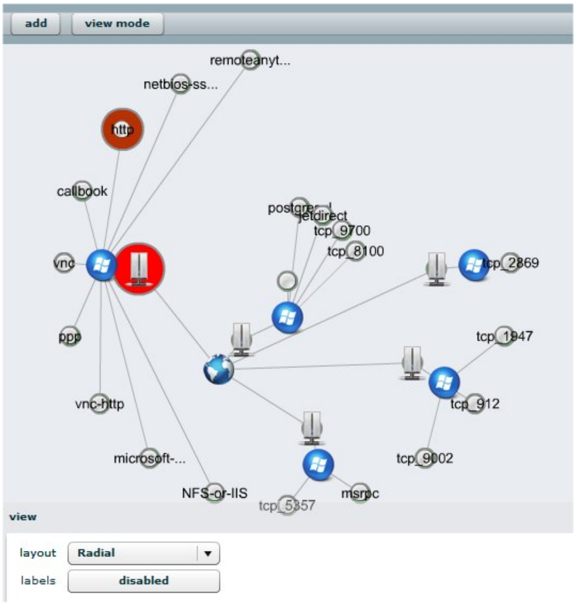


ALERT:
http **is threaten by:**
- Attacker_can_execute_arbitrary_code_within_the_LocalSystem_security_context (v:web_server_is_affected_by_a_buffer_overflow)

layout Radial

labels disabled

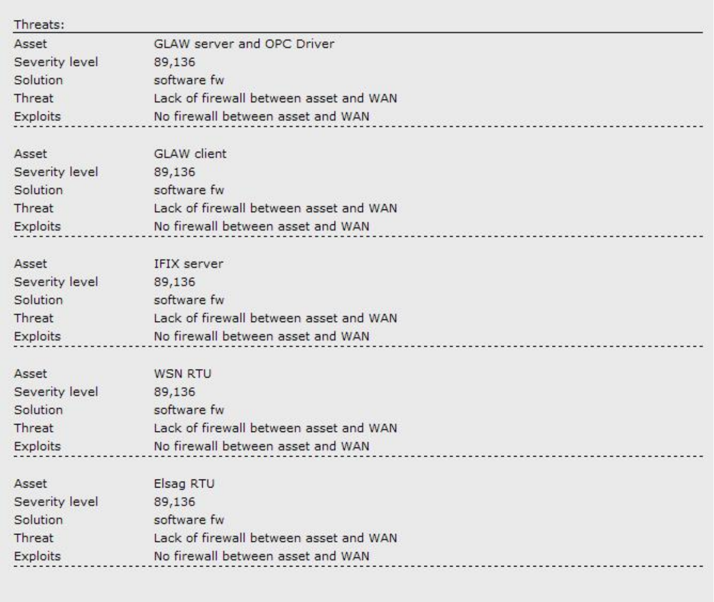
Fig. 8. Topology diagram and visualized threatened nodes



layout: Radial

labels: disabled

Fig. 9. Topology diagram and visualized threatened nodes after installing the firewall and anti-virus applications



Threats:

Asset	GLAW server and OPC Driver
Severity level	89,136
Solution	software fw
Threat	Lack of firewall between asset and WAN
Exploits	No firewall between asset and WAN
Asset	GLAW client
Severity level	89,136
Solution	software fw
Threat	Lack of firewall between asset and WAN
Exploits	No firewall between asset and WAN
Asset	IFIX server
Severity level	89,136
Solution	software fw
Threat	Lack of firewall between asset and WAN
Exploits	No firewall between asset and WAN
Asset	WSN RTU
Severity level	89,136
Solution	software fw
Threat	Lack of firewall between asset and WAN
Exploits	No firewall between asset and WAN
Asset	Elsag RTU
Severity level	89,136
Solution	software fw
Threat	Lack of firewall between asset and WAN
Exploits	No firewall between asset and WAN

Fig. 10. Security report with the ranked threats

At the beginning of the demo the system topology is analyzed. The example topology of our test bed can be shown in Fig. 7. The arrow indicated the router where firewall and anti-virus applications will be turned off. As is it shown in Fig. 8 single action has impact on many nodes being in relation with affected router. The cascading effect can be noticed. Turned off firewall and anti-virus protection exposes the W2K operating systems to different network attacks, which eventually has impact on the provisioning of the applications hosted by that OS. What is more it is also assumed that the IIS WWW server with WebDav service is enabled on W2K OS (default configuration is assumed due to the lack of detailed information about ran applications and services). The majority of discovered problems can be solved by installing anti-virus and firewall applications on W2K OS. Therefore the user inserts into DAT the information that such an action has been taken and as result new security report is obtained (the visualized topology can be shown in Fig. 9).

5 Conclusion

In this paper, the fusion of the ontology-based approach and the Bayesian network is proposed. Such innovative solution is applied in Decision Aid Tool for critical infrastructures security status assessment.

The sample result of CI system security evaluation by DAT is presented in Figure 10. The presented security report contains the ranked threats for discovered assets with their threat severity value calculated by the Bayesian network. Moreover, in the security report, details about the detected threats and the proposed solutions are given.

Acknowledgment

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 225553 (INSPIRE Project).

References

1. European Parliament legislative resolution of 10 July 2007, on the proposal for a Council directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection (COM(2006)0787 C6-0053/2007 2006/0276(CNS)) (July 2007)
2. XiaoFeng, D., YuJiong, G., Kun, Y.: Study on Intelligent Maintenance Decision Support System Using for Power Plant Equipment. In: Proc. of the IEEE International Conference on Automation and Logistics Qingdao, China, 96100 (September 2008)
3. Lee, S.J., Mo, K., Seong, P.H.: Development of an Integrated Decision Support System to Aid the Cognitive Activities of Operators in Main Control Rooms of Nuclear Power Plants. In: Proc. of IEEE Symposium on Computational Intelligence in Multicriteria Decision Making (MCDM), pp. 146–152 (2007)

4. Zhang, B., Wu, G., Shang, S.: Research on Decision Support System of Water Pollution Control Based On Immune Agent. In: Proc. of International Symposium on Computer Science and Computational Technology, ISCSCT, vol. 1, pp. 114–117 (2008)
5. Xie, L., Wang, Z., Bian, L.: The Research of Oileld Flood Precaution Decision Support System. In: Proc. of International Seminar on Business and Information Management, ISBIM 2008, vol. 2, pp. 236–239 (December 2008)
6. ISO/IEC 13335-1:2004, Information Technology Security Techniques Management of information and communications technology security Part 1: Concepts and models for information and communications technology security management (2004)
7. Choras, M., Stachowicz, A., Kozik, R., Flizikowski, A., Renk, R.: Ontology-based approach to SCADA systems vulnerabilities representation for CIP. Electronics 11, 35–38 (2009)
8. Choras, M., Flizikowski, A., Kozik, R., Renk, R., Holubowicz, W.: Ontology-Based Reasoning Combined with Inference Engine for SCADA-ICT Interdependencies, Vulnerabilities and Threats Analysis. In: Pre-Proc. of 4th International Workshop on Critical Information Infrastructures Security, CRITIS 2009, Bonn, Germany, pp. 203–214. Fraunhofer IAIS (2009)
9. SWRL: A Semantic Web Rule Language Combning OWL and RuleML, W3C Member Submission, `http://www.w3.org/Submission/SWRL/`
10. Deliverable D2.3, Ontological approach and inference engine, INSPIRE Project (2009)
11. Macaulay, T.: Critical infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies (August 2008)
12. Lewis, T.G.: Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley-Interscience, Hoboken (2006)
13. McClanahan, R.H.: The benefits of networked SCADA systems utilizing IP-enabled networks. IEEE, Los Alamitos (2002)

OMEGA: New Use Cases for Future Home Networks

Jean-Philippe Javaudin[1], Martial Bellec[1],
Gilles Goni[1], and Rafael Gonzalez Fuentetaja[2]

[1] Orange Labs, France Telecom
Cesson Sévigné, France
{jeanphilippe.javaudin,
martial.bellec,gilles.goni}@orange-ftgroup.com
[2] Telefonica I+D
Madrid, Spain
rfg@tid.es

Abstract. The media richness of the services available to the end consumer has had a constant increase rate of about 8% per year over the last century. This leads nowadays to the need of Ultra Broadband at home to handle future services such as 3D. Ultra Broadband means bit rates reaching the Gigabit per second. Moreover, beyond the bandwidth increase, the home network capabilities have to evolve in order to support new usages. This paper describes typical usage scenarios for the next 2-3 years and derives network oriented use cases that serve as requirements for the home network. Finally a solution fulfilling these requirements, based on an inter-MAC convergence layer, is depicted. This solution is developed in the OMEGA FP7 project.

Keywords: Home area networks, network convergence, Inter-MAC, network architecture.

1 Introduction

Current and future services and contents in home area networks (HANs) put diverse demands on the underlying transmission technology. For example, the use case scenarios for future home networks require an overall network capacity up to the Gigabit per second (Gbps). Moreover in order to avoid inefficient and cumbersome solutions with coexistence problems as experienced today, the OMEGA project [1-3] integrates various appropriate technologies into a converged heterogeneous network (see Fig. 1), which meets the customer's demands with respect to quality of service, reliability, throughput, ubiquity, and self-configuration.

From a race to Gbps perspective,

- the multitude of radio systems operating in a single home network and using the overcrowded frequency bands will create coexistence and performance problems. Convergence at the radio level will consequently be a key concept to be investigated.
- Technological enhancements will be investigated in order to locally optimize the different wireless technologies so that they provide the required performance in a converged network.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 464–471, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

  - In order to meet a full coverage of the home, combination with other technologies such as powerline or wireless optical communications are necessary.

Then, from a quality of service point of view:

- Wireless connectivity with Gbps is not QoS achievable within more than one room
- From a network perspective, IP layer cannot mitigate PHY impairments to QoS acceptance while still being the de facto standard for the connected home.
- Additionally the home network power consumption should be limited. The reasons are twofold: reducing the operational cost of the network for the user and provide a sustainable component to home networks.

From a simplicity point of view:

- Electrical sockets are the most convenient medium term way to bring wire line connectivity in Europe.
- The final link of the in-house communication will preferably be wireless.
- The end customer will have the final word!

In this paper we present in section 2 typical usages of the home network, exemplified by a family composed of four members. These usages are then derived into requirements on the home network. Then we also highlight in section 3 other requirements for the home network as developed in the OMEGA project. Section 4 depicts a solution investigated in the OMEGA project in order to make converge all kind of physical technologies into one coherent framework. OMEGA partners are developing an evolutionary solution based on the Inter-MAC concept to accommodate these challenges by elaborating a minimum upper interface (namely the middleware south interface). Section 4 also explains the reference architecture of the OMEGA network.

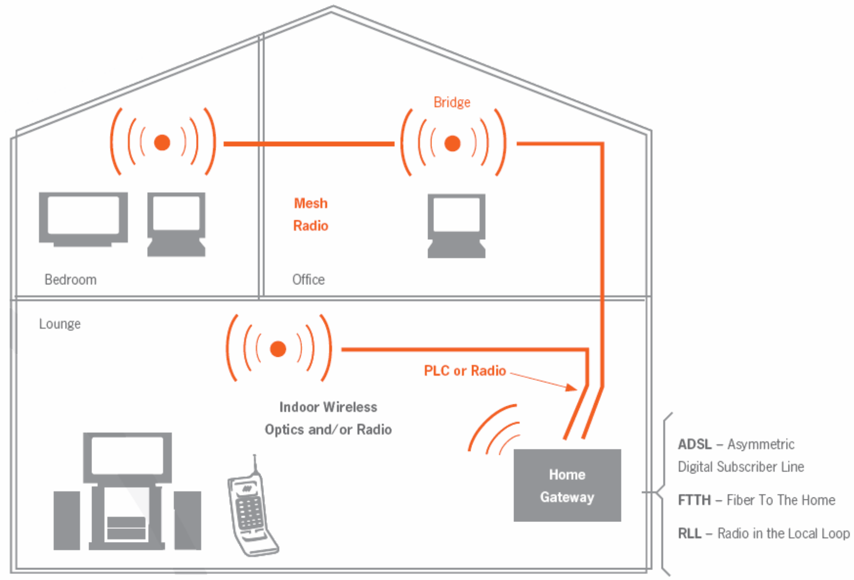


Fig. 1. Gigabit home area network: OMEGA concept

2 Use Cases

2.1 Typical Family Usage of the Home Network

Some scenarios have been defined in the OMEGA project, see [4–6]. These scenarios involve a family of 4 persons at different periods of the day. See for instance on Fig. 2 a representation of the early morning as all family members are still in their respective bedrooms:

- parents are listening music,
- the girl is looking at TV the end of the program from the previous evening,
- the boy is checking his downloads status.

All these flows run in parallel in the home network, which shall convey them while guaranteeing their respective Quality of Service. In the same family, the girl is giving a phone call in the afternoon while moving in the home and enjoying a seamless connection from a room to another. More details on these scenarios are captured in [4–6].

In the next section we derive these usage scenarios into network oriented use cases. These use cases serve as requirements for the definition of home network functionalities.

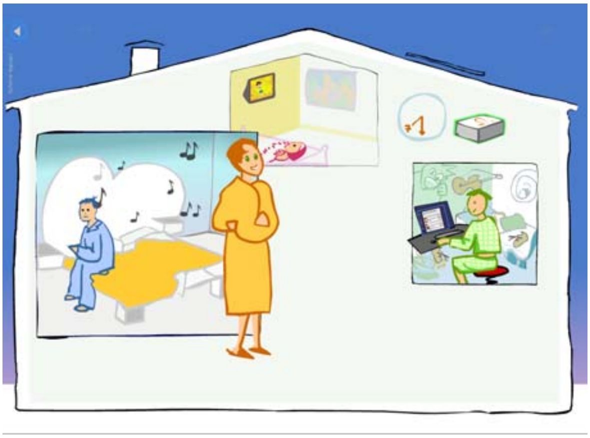


Fig. 2. Use of simultaneous very high bit rate flows within the home, with guaranteed QoS

2.2 Derivation of the Usage to Network Oriented Requirements

The list of requirements for the network that can be derived from the scenarios above are:

1. Always best connected in the home: When multiple connectivities are available between a source and a destination the network shall automatically select the best one to guarantee the QoS. This shall be transparent both for the user and for the application level in the network.
2. Exploit the whole network: the network shall allow the use of multiple links in parallel from a source to the same destination, either split of the traffic flow by flow or even split a single flow.

3. Mobility: the nomadism of a terminal in the home network shall be made possible, in a seamless way, regardless of the connectivities
    a. Intra-techno (Wifi 2.4 GHz / 5 GHz)
    b. Inter-techno (Wifi/wireless optics ...)
4. Ubiquitous coverage in the home network: Not to increase extensively the network elements in the home, future end devices shall act as network extenders by relaying the flows.
5. Compatibility with legacy: all devices already on the market shall be supported and their performance shall not be degraded.

Figure 3 to figure 5 present use cases that illustrate some of these requirements.

3 Further Requirements for the Home Networks

3.1 Compatibility with Future Access Networks

Another major concern for the architecture is the fact that the OMEGA home network design should keep in mind continuity of the access network to a certain extent. The home gateway is commonly considered as the border network element between the home network and the access provider network. This does not imply that there may not exist some continuity between these two network segments. On the opposite, one of the purposes of the OMEGA architecture is also to highlight how the evolutions expected in the access network may impact the operation of the OMEGA home. Deep evolutions are expected in the operator access and regional network, even if their roadmap is slower than that of the area of home networking:

- the dramatic increase of the data rates in the access and, as a result of this fact, the emergence of optical fibre in the access, likely up to the client's premises, with the prospect of reusing the potential of that technology in the Gigabit home network,
- a packet oriented handling of the QoS,
- the emergence of an IPv4/IPv6 coexistence, with the prospect of some simplification of the configuration process of the client installation,
- the emergence of an integrated IMS as a new (SIP based) intelligent network based on an IP network,
- the consolidation of new powerful means of management of large scale networks.

Therefore, one clear ambition of the OMEGA architecture is to assess the impact of these evolutions on the organization of the Gbps home area network, and how the protocols implemented in the access/regional network can be profitably extended in that context. These aspects will be elaborated in a later stage of the OMEGA project.

3.2 Compatibility with Future Middleware

A common definition is that middleware is the "glue" between software components or between the software and the network. The goal of the middleware is therefore to make different devices inter-work for the delivery of the service to the end user and thus its main goal is to hide the complexity of the inter-working devices under the service layer and abstracting it from the physical evidence of the home network. Several middleware solutions already exist: UPnP/DLNA, DPWS, IGRS, BONJOUR, HAVI, but they are not interoperable. There is no standardised and widely accepted middleware standard so far, while the IP layer is addressing some of the middleware core functions as a pivot convergent technology.

In this context, the task for OMEGA will be to elaborate a minimum upper interface (namely the middleware south interface) in order to provide:

- the requesting/maintaining/releasing of service flows,
- guaranteed QoS requirements to these flows, and report limitations, instantaneously, to the middleware so that relevant means are taken by the application (renegotiating the QoS in a SIP/SDP-like way or even dropping the flow),
- easy local or remote management given a top level view to the end user or the ISP.

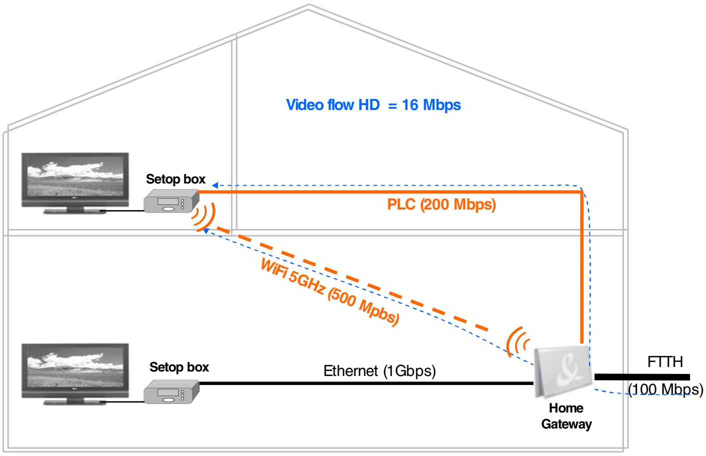


Fig. 3. Illustration of the use case "selection of the best link"

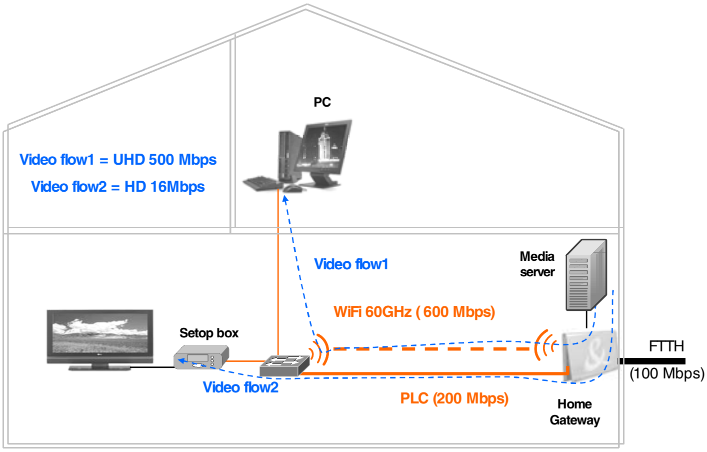


Fig. 4. Illustration of the use case "using all links"

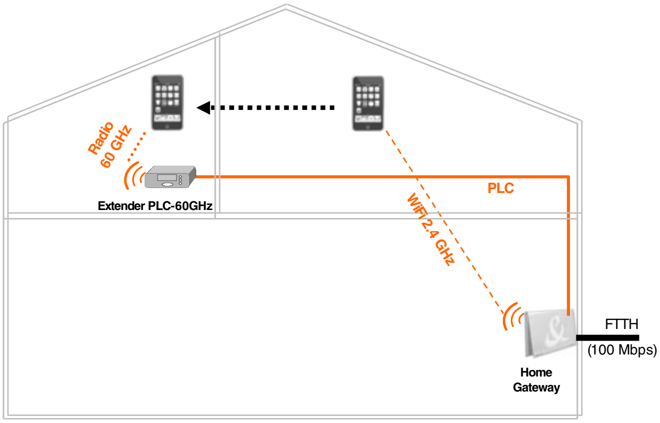


Fig. 5. Illustration of the use case "nomadism inter-technology"

4 Network Architecture and Inter-MAC Convergence

4.1 Main Goal

In order to fulfil the requirements on the home net works listed in section 2, the OMEGA project developed a Layer 2.5 solution so-called Inter-MAC. The Inter-MAC layer [8] may be seen as a global resource manager over the heterogeneous technologies in use in the HAN. To achieve that goal it plays the role of adapter between the logical links and the network layer. It operates at Layer 2, as shown in Fig. 6, but it is technology-independent and uses the information received from the underlying technologies to select the most appropriate one fitting to services requirements. The Inter-MAC is able to control every communication between two and more devices in the home network, with functionalities such as path selection or technology handover. The Inter-MAC interacts with the signalling, the management and the data plane to transparently setup a home network giving a sensation to the applications that the home network is a unique and homogeneous technology and not a cooperation of extremely different communication technologies. Thus, the Inter-MAC convergence layer integrates arbitrary heterogeneous communication technologies in a single home network.

4.2 Inter-MAC Connectivity

Thanks to the Inter-MAC layer, the OMEGA network, from an IPv4/IPv6 point of view, is a unique local area network (LAN). No layer 3 routing is needed within an OMEGA network. The frames/packets are forwarded to the correct destination node thanks to a path selection algorithm.

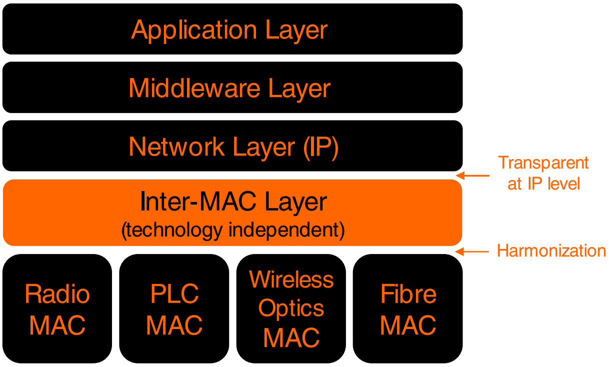


Fig. 6. Inter-MAC Layer in the OSI protocol stack

4.3 Reference Architecture Model and Interfaces

The Inter-MAC concept applies to a set of OMEGA devices constituting the OMEGA network which is organized in the form of a mesh architecture bringing in the advantages of multi-path capabilities for traffic reconfiguration. Their association can be represented under the global name of "OMEGA device", keeping apart the OMEGA gateway in order to highlight the interface with the access network. This leads to the OMEGA architecture reference model presented in Fig. 7, additional details about OMEGA architecture can be found in [7]. In a real network, several end devices, extenders and legacy device adapters can be interconnected in a ramified and extensive way. Then, the OMEGA network can be considered as a set of OMEGA devices, i.e. devices implementing the Inter-MAC layer described in the previous section. We refer hereafter as *legacy* the devices connected to the home network but not implementing the Inter-MAC.

Fig. 7 shows all the interfaces of the OMEGA architecture reference model. For simplicity, only one OMEGA device is shown. It represents a multitude of OMEGA devices connected by Ω links with Ω interfaces in a mesh topology. By reference to the documents from the ITU-T and from the Broadband Forum, the *U interface* is defined as the interface providing connectivity between the OMEGA network and the access network. The U interface relies on a broadband access technology, for instance, ADSL2+, VDSL2, FTTH GPON, CATV or WiMAX. In the same way, the *R interface* is defined as the interface ensuring the connection of legacy devices and networks (which do not support the Inter-MAC framework) to the OMEGA network. The R interface may rely on various home networking technologies such as USB, SCART, IEEE1394, Wi-Fi, UWB or Bluetooth.

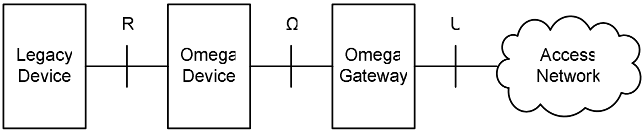


Fig. 7. Interfaces of OMEGA Architecture Reference Model

5 Conclusion

This paper describes the key challenges a home area network able to support future usages. These are exemplified by a typical 4 person's family. This implies an increase of the network bandwidth and a convergence among technologies to achieve seamless handovers and ubiquitous coverage in a heterogeneous environment.

We also explained how the inter-MAC solution and associated architecture proposed in the OMEGA European project is felt as one of the most promising solutions for the future.

All project results are captured in a number of public deliverables to disseminate these findings [1]. The OMEGA project is now ready to come to hardware/software design to produce an initial prototype of convergent home network in 2010. More advanced features will be simulated and evaluated so that a second version of the project prototype with advanced functionalities will become a reality before end of 2010.

Acknowledgement

Part of the research leading to these results has received funding from the European Community's Seventh Framework Programme FP7/2007-2013 under grant agreement n° 213311 also referred as OMEGA.

References

1. ICT OMEGA project website, `http://www.ict-omega.eu`
2. OMEGA White Paper, Inter-MAC Concept for Gb/s Home Network (April 2009) (available on project website)
3. Javaudin, J.-P., Bellec, M., Varoutas, D., Suraci, V.: OMEGA ICT Project: Towards Convergent Gigabit Home Networks. In: PIMRC 2008 Conference, Cannes, September 15-18 (2008)
4. ICT OMEGA project deliverable D1.1, Final Usage Scenario report (September 2008), `http://www.ict-omega.eu/publications/deliverables.html`
5. ICT OMEGA project deliverable D1.4, Requirements, Architecture and Topology report (October 2009), http://www.ict-omega.eu/publications/deliverables.html
6. ICT OMEGA project deliverable D7.2, Platform – Service specifications (September 2009), `http://www.ict-omega.eu/publications/deliverables.html`
7. ICT OMEGA project deliverable D6.1, OMEGA Architecture Reference Model (December 2008), `http://www.ict-omega.eu/publications/deliverables.html`
8. ICT OMEGA project deliverable D5.3, Inter-MAC protocol entities interfances specifications (September 2009), `http://www.ict-omega.eu/publications/deliverables.html`

Adaptive Filter Bank Modulation for Next Generation Wireless In-Home Networks*

Salvatore D'Alessandro and Andrea M. Tonello

Università degli Studi di Udine, via delle Scienze 208, 33100 Udine – Italy
{`salvatore.dalessandro,tonello`}@uniud.it

Abstract. In this paper we investigate the deployment of filtered multitone (FMT) modulation over in-home wireless channels. We propose the adaptation of parameters (overhead factor) to the channel condition. Optimal and sub-optimal approaches are described. Comparisons with orthogonal frequency division multiplexing (OFDM) show that FMT provides significant improvements both in single user and multi user (based on frequency division multiplexing) cases.

Keywords: OFDM, Filtered Multi-Tone, OFDMA, WLAN, IEEE 802.11, Adaptive Cyclic Prefix, Adaptive Overhead.

1 Introduction

In multi carrier modulation (MCM) systems, a broadband signal is split into M narrow band signals such that each of them experiences a near flat frequency response. This idea simplifies the equalization task, namely, the mitigation of the inter-symbol interference (ISI) caused by the channel frequency selectivity, and allows approaching the channel capacity making use of bit and power loading techniques [1]. Beside, considering the multi user scenario, the M sub-channels of a MCM scheme can be optimally partitioned among the network users realizing the so called frequency division multiple access (FDMA).

A MCM system can be described using a filter bank architecture [2]. In such a case, at the transmitter side, the M parallel data signals are interpolated by a factor $N = M + \beta$, filtered with a modulated prototype pulse and transmitted over the channel. The interpolation factor (IF) N, or equally the overhead (OH) β, and the modulated prototype pulse determine the type of MCM scheme, e.g., OFDM or FMT. On the other hand, the IF also affects the achievable rate of the system. As an example, in OFDM, the IF determines the duration of the cyclic prefix (CP). As it is well known, if the CP is longer than the channel duration, the received signal will be neither affected by inter-carrier interference (ICI) nor by ISI [3]. Nevertheless, this benefit is paid in terms of a loss in achievable rate

---

* The work of this paper has been partially supported by the European Community's Seventh Framework Programme FP7/2007-2013 under grant agreement n. 213311, project OMEGA – Home Gigabit Networks.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 472–483, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

and in signal over noise ratio (SNR) of a factor $M/(M+\beta)$, with β equal to the CP duration.

In our previous work [4], we have found that over typical WLAN channels, the CP has not to be necessarily long as the channel duration to maximize the achievable rate, or with an abuse of terminology, to maximize capacity. Furthermore, for each channel class of the IEEE 802.11n WLAN channel model [5], we have found a near optimal value of CP designed according to the statistic of the capacity-optimal CP duration. We have shown that capacity improvements for the WLAN standard are attainable adapting the CP to the experienced channel class, this is true for both the single and the multi user cases. Moreover, for the multi user case, we have found that the CP adaptation to the channel class improves the aggregate network rate either with the use of orthogonal FDMA (OFDMA) or with the use of time division multiple access (TDMA).

In [6] it has been shown that for the single user case, over typical power line channels, FMT provides significant gains in terms of achievable rate w.r.t. OFDM. This statement is true considering both FMT and OFDM with OH adapted to the channel conditions.

Inspired by the above results, in this paper we are interested on extending to the FMT the approach followed in [4] to design the OH in OFDM. That is, in this work we find a limited set of OH values for FMT using the statistic of the capacity-optimal OH. The set of OH values is used to adapt the system to the channel conditions. We call such a system adaptive-FMT. We compare adaptive-FMT with adaptive-OFDM presented in [4] and we show that further capacity improvements to the IEEE 802.11 standard could be obtained adopting the former scheme.

Regarding the multi user case, we focus on the downlink channel where the access point (AP) signals to the N_U users of the network. Considering this scenario, we propose for FMT-FDMA a sub-channel allocation algorithm jointly with the adaption of the OH duration. We then compare adaptive-FMT-FDMA with adaptive-OFDMA (presented in [4]) and we show that the former scheme significantly outperforms the latter.

The paper is organized as follows. In Section 2 we introduce the general MCM scheme as a filter bank architecture. Thus, considering a single user scenario, in Section 3 we compute the optimal and the sub-optimal OHs for both FMT and OFDM. In Section 4, we extend the OH adaptation to the multi user case, namely, to FMT-FDMA and to OFDMA.

Extensive numerical results that compare FMT and OFDM in both single and multi user cases are presented in Section 5. Finally, the conclusions follow.

2 System Model

We consider the downlink channel from the AP to the N_U users of the network. The M parallel data signals of user u are denoted with $a^{(u,k)}(\ell)$, $k = \{0, \ldots, M-1\}$, $\ell \in \mathbb{Z}$. Each data signal is interpolated by a factor N, filtered with a sub-channel pulse $g(n)$, and modulated by the k-th sub-carrier $f_k = k/M$. For both

OFDM and FMT the sub-carrier modulation is accomplished via an exponential function. Therefore, the base-band discrete-time multicarrier signal for user u can be written as the output of a synthesis filter bank, i.e.,

$$x^{(u)}(n) = N \sum_{k \in \mathbb{K}^{(u)}} \sum_{\ell \in \mathbb{Z}} a^{(u,k)}(\ell) g(n - \ell N) e^{j2\pi f_k n}, \tag{1}$$

where $\mathbb{K}^{(u)}$ denotes the set of sub-channels indices assigned to user u. Clearly, $\mathbb{K}^{(u)} \subseteq \{0, \ldots, M-1\}$.

The signal is transmitted from the access point to the user u over a channel that has an equivalent complex impulse response $g_{ch}^{(u)}(n,d)$, where d denotes the distance between the transmitter and the receiver. As it was assumed in our previous work [4], also here we use the IEEE 802.11 TGn channel model [5]. We just recall that this model generates channels belonging to five classes labeled with B,C,D,E,F, and that each class is representative of a certain environment, e.g., small office, large open space/office with line of sight (LOS) and non LOS (NLOS) propagation, and so on. For a description of the channel model used through this work, please see [4], [5].

The received signal $y^{(u)}(n) = x^{(u)}(n) * g_{ch}^{(u)}(n,d)$ is analyzed with a filter bank having sub-channel pulses $h(n)$. The outputs are sampled with period N. Therefore, before equalization, the signal received by user u in the k-th sub-channel is given by

$$z^{(u,k)}(\ell) = a^{(u,k)}(\ell) g_{TOT}^{(u,k)}(0) + ISI^{(u,k)}(\ell) + ICI^{(u,k)}(\ell) + \eta^{(u,k)}(\ell) \,. \tag{2}$$

In (2), $g_{TOT}^{(u,k)}(0)$ denotes the complex amplitude of the data of interest, whereas, $ISI^{(u,k)}(\ell)$, $ICI^{(u,k)}(\ell)$, and $\eta^{(u,k)}(\ell)$ respectively denote the ISI, the ICI and the noise term experienced by user u in sub-channel k. The interference terms are in general present when transmitting through a frequency selective channel. They can be mitigated with some form of equalization. The filter bank design aims at reaching a tradeoff between ISI and ICI. While the presence of both ISI and ICI requires a multi-channel equalizer, the presence of only ISI allows using sub-channel equalization. In our analysis we consider the use of sub-channel equalization only. Therefore, the signal after the sub-channel equalization can be written as

$$z_{EQ}^{(u,k)}(\ell) = a^{(u,k)}(\ell) g_{EQ}^{(u,k)}(0) + ISI_{EQ}^{(u,k)}(\ell) + ICI_{EQ}^{(u,k)}(\ell) + \eta_{EQ}^{(u,k)}(\ell) \,, \tag{3}$$

where we use the subscript EQ to denote the dependence from the equalizer. The terms $g_{EQ}^{(u,k)}(0)$, $\eta_{EQ}^{(u,k)}(\ell)$, $ISI_{EQ}^{(u,k)}(\ell)$ and $ICI_{EQ}^{(u,k)}(\ell)$, respectively denote the peak of the overall impulse response, the noise term and the interference terms at the k-th sub-channel equalizer output.

In the next sub-sections we derive the OFDM and the FMT MCM schemes.

OFDM. The OFDM scheme can be obtained setting the synthesis and the analysis pulses respectively equal to

$$g(n) = \frac{1}{N} rect\left(n/N\right), \qquad h(n) = \frac{\sqrt{N}}{M} rect\left(-(n+\beta)/M\right), \tag{4}$$

where $rect\,(n/A) = 1$ for $n = \{0, 1, \ldots, A-1\}$ and zero otherwise. The factor β denotes the length of the CP. As previously said, when the length of the CP is greater than the channel duration, the received signal (2) is neither affected by ISI nor by ICI [3]. In such a case the equalization task reduces to a simple single tap zero forcing sub-channel equalizer. Through this work, when showing numerical results for OFDM, we assume the use of a simple single tap sub-channel equalizer. That is, each sub-channel equalizer multiplies the received signal (2) by $\left(g_{TOT}^{(u,k)}(0)\right)^{-1}$. We make this assumption to maintain simple the OFDM implementation.

FMT. FMT was originally proposed for application in very high speed digital subscriber lines (VDSL) [7]. Then, studied for multi user wireless communications in [8]. Recently, it has been investigated for power line channels [6,9]. In FMT the sub-channel symbol period is N and the analysis pulse is matched to the synthesis pulse, i.e., $h(n) = g^{(*)}(-n)$. A distinctive characteristic of FMT is that the prototype pulse is designed to obtain high frequency confinement [7]. Therefore, qualitatively we can say that in FMT the ICI term is negligible, and thus the equalization task focuses on deleting the ISI term. This observation justifies our assumption of considering only sub-channel equalization.

When showing numerical results for FMT, we consider MMSE fractionally spaced sub-channel equalization [10]. Furthermore we deploy truncated root-raised-cosine pulse with rolloff equal to $(N-M)/M$, and length 10 symbols to obtain good frequency confinement.

3 Adaptive Overhead: The Single User Case

In this section we first recall the method used in [6] to optimally adapt the OH of OFDM and FMT to the channel realization. Then, we briefly recall the method proposed in [4] to adapt the CP of OFDM to the experienced channel class of the 802.11n channel model [5]. Finally, making the proper adjustments, we extend this last method to FMT.

3.1 Optimal OH Adaptation

In order to evaluate the impact of the OH duration on the system performance we compute the capacity assuming parallel Gaussian channels. That is, we assume additive white Gaussian noise, independent and Gaussian distributed input signals, which renders ISI and ICI also Gaussian (cf. e.g. [3]). The capacity in bit/s for the link of user u and for a given channel realization is given by

$$C^{(u)}(\beta) = \sum_{k \in \mathbb{K}^{(u)}} C^{(u,k)}(\beta), \tag{5}$$

with

$$C^{(u,k)}(\beta) = \frac{1}{(M+\beta)T} \log_2\left(1 + SINR_{EQ}^{(u,k)}(\beta)\right), \tag{6}$$

where $SINR_{EQ}^{(u,k)}(\beta)$ denotes the signal over interference plus noise ratio, after sub-channel equalization, experienced by user u in sub-channel k when we transmit using an OH of β samples. Details on its computation, for OFDM, can be found in [11].

In (5), the factor T denotes the system sampling period. Through this work we assume to transmit power across sub-channels at a constant level given by a constraint on the power spectral density (PSD).

From (5), we can see that the capacity of both OFDM and FMT is a function of the OH duration β. Therefore, considering a single link communication, the optimal approach to adapt the OH to the channel realization is to choose β as such value that maximizes capacity (5), i.e.,

$$\beta_{opt}^{(1)} = \underset{0 \leq \beta < \nu^{(1)}}{\operatorname{argmax}} \left\{ C^{(1)}(\beta) \right\}, \tag{7}$$

where we have denoted with $\nu^{(1)}$ the channel duration in samples.

Since the argument of (7) is generally not convex, the implementation of the optimal approach to adapt the OH to the channel realization requires an exhaustive search which is complex.

A significant simplification that assures the feasibility of the OH adaptation to the channel realization, is to pre-compute a limited amount of OH values, and then adapt the OH over this small set of values. This is discussed in the next sub-section.

3.2 Simplified OH Adaptation

In this section we are interested at finding a finite set of OH values over which perform adaptation. The method that we use is based on the evaluation of the statistic of the capacity-optimal OH (7). As it will be clarified in the following, since the statistic of the capacity-optimal OH depends on the used MCM scheme, in the following we distinctly describe the simplified OH adaptation for OFDM and FMT.

Simplified OH Adaptation in OFDM. To determine the limited set of CP values for OFDM, in [4] we have proposed an approach based on the evaluation of the cumulative distribution function (CDF) of the capacity-optimal CP (7). The numerical results (see Section 5) show that the capacity-optimal CP value depends on the specific channel realization and therefore, in general, it relies on the channel class and on the distance between the AP and the user. However, we have noted that the CP value variations are more pronounced among classes than within a given class. That is, the variation of the CP for the channel realizations of a given class for various distances is not as significant as if we draw channels from different classes. Hence, we have proposed to choose a single value of CP for all channel realizations that belong to a certain channel class. For a given class and distance, the specific CP length is chosen to be the value of β for which the CDF of (7) is 99%. Then, to obtain a single CP value associated to that class we pick the largest CP among those obtained for the considered set of distances, say from 3 m to 60 m. The set of the obtained CP values for the five classes is denoted with $\mathbb{P}_{OFDM} = \left\{\beta^{(99\%)}_{B,OFDM}, \beta^{(99\%)}_{C,OFDM}, \beta^{(99\%)}_{D,OFDM}, \beta^{(99\%)}_{E,OFDM}, \beta^{(99\%)}_{F,OFDM}\right\}$.

Clearly, once the devices know the scenario in which they are working, or equivalently the experienced channel class, the CP adaptation reduces to pick the corresponding value of CP from the set $\mathbb{P}_{OFDM}$.

Simplified OH Adaptation in FMT. To determine the limited set of OH values for FMT, we use a method similar to the one above described for OFDM.

Looking at the capacity-optimal OH CDFs of FMT (see Section 5), we notice that its variations are more pronounced within a given class than among different classes. In other words, the capacity-optimal OH CDF of FMT strongly relies on the distance between transmitter and receiver. Whereas, for a given distance, the dependence among classes is negligible. Therefore, for FMT we choose to define the limited set of OH values based on the distance between transmitter and receiver. In order to have a limited set of OH values, we compute the capacity-optimal OH CDF only for four values of distances, i.e., 3 m, 10 m, 30 m, 60 m. Now, for each value of distance, we choose a near optimal OH as the value of OH that renders the corresponding capacity-optimal OH CDF equal to 99%. The corresponding set of OH values is $\mathbb{P}_{FMT} = \left\{\beta^{(99\%)}_{3,FMT}, \beta^{(99\%)}_{10,FMT}, \beta^{(99\%)}_{30,FMT}, \beta^{(99\%)}_{60,FMT}\right\}$.

Differently from OFDM, in this case even if the devices know the scenario where they are working (or equally the experienced channel class) the choice of the OH requires an exhaustive search over the values of OH belonging to $\mathbb{P}_{FMT}$. Therefore, $\beta^{(1)}_{opt} = \mathrm{argmax}_{\beta \in \mathbb{P}_{FMT}} \left\{C^{(1)}(\beta)\right\}$.

It is worth noting that for FMT, if we chose for each channel class, the smallest value of β such that all the OH CDFs are lower than 0.99, as we did for OFDM, we would obtain the same OH value for all the channel classes. Thus, this method could be used to design a single value of OH in FMT.

4 Adaptive Overhead: The Multi User Case

Since we have already shown in [4] that OFDMA outperforms OFDM that deploys time division multiple access, to assess the performance of multiuser FMT we consider a network where multiplexing is accomplished via FDMA. Therefore, depending on the considered MCM scheme we have FMT-FDMA and OFDMA. We focus on the downlink channel from the AP to the N_U users of the network. Since the channels experienced by the users are different, the AP allocates the sub-channels and the OH according to a fair principle based on maximizing the aggregate network rate but assuring that all users exceed a minimum rate.

In the following we extend to the case of FMT-FDMA the optimal and the sub-optimal OH and sub-channels allocation algorithms that we have described in [4] for OFDMA.

4.1 Sub-channels and OH Adaptation

In order to allocate the sub-channels to the network users, for a certain value of β, the AP can solve the following optimization problem

$$R(\beta) = \max_{\underline{\alpha}} \sum_{u=1}^{N_U} \sum_{k \in \mathbb{K}} \alpha^{(u,k)} C^{(u,k)}(\beta), \quad \text{s.t.} \sum_{u=1}^{N_U} \alpha^{(u,k)} = 1, \quad k \in \mathbb{K},$$
$$\sum_{k \in \mathbb{K}} \alpha^{(u,k)} C^{(u,k)}(\beta) \geq p^{(u)} \sum_{k \in \mathbb{K}} C^{(u,k)}(\beta), \quad u = 1, ..., N_U. \tag{8}$$

In (8), $\alpha^{(u,k)}$ denotes the binary sub-channel coefficient equal to 1 if sub-channel k is allocated to user u, and to zero otherwise, and $\underline{\alpha} = \{\alpha^{(u,k)}$, for $u = 1, \ldots, N_U$; and $k \in \mathbb{K}\}$. $p^{(u)}$ are quality of service coefficients, each indicates the percentage of achievable rate that the u-th user has to achieve w.r.t. the one that it would achieve in the corresponding single user scenario. $R(\beta)$ denotes the aggregate network rate when deploying an OH of β samples. $\mathbb{K}$ denotes the set of available sub-channels, e.g., for the WLAN standard [12], it corresponds to $M = 64$ sub-channels deployed in a frequency band of 20 MHz. Problem (8) can be solved using integer programming (IP) [13]. In order to diminish the computational complexity, we solve (8) via linear programming (LP) followed by rounding the coefficients $\alpha^{(u,k)}$ to the nearest zero or one integer. Consequently, for each value of β the set of sub-channels assigned to user u is given by $\mathbb{K}^{(u)} = \{k : \alpha^{(u,k)} = 1\}$. The optimal value of β is obtained by the maximization: $\text{argmax}_{\beta} \{R(\beta)\}$.

The exhaustive search of the OH values renders the algorithm complexity relatively high. A significant simplification is obtained if we solve (8) with LP only for the finite set of OH values that has been pre-determined in the single user case according to the criteria of Section 3.2. That is, the optimal OH is respectively given by $\beta_{\text{opt}}^{OFDMA} = \text{argmax}_{\beta \in \mathbb{P}_{OFDM}} \{R(\beta)\}$ for OFDMA, and by $\beta_{\text{opt}}^{FMT-FDMA} = \text{argmax}_{\beta \in \mathbb{P}_{FMT}} \{R(\beta)\}$ for FMT-FDMA.

It is worth noting that for the case of OFDMA, if the environment where the devices operate is known, or in other words, the AP knows the channel class of its network, the set $\mathbb{P}_{OFDM}$ of the CPs reduces to one value. Therefore, for OFDMA, the allocation of sub-channels to the network users consists in solving (8) only for a single value of β.

5 Numerical Results

To obtain numerical results, we have chosen the following system parameters that, considering OFDM, are essentially those of the IEEE 802.11 standard [12]. The MCM systems use $M = 64$ sub-channels with a transmission bandwidth of 20 MHz. The signal is transmitted with a constant power spectral density (PSD) of -53 dBm/Hz. At the receiver side, we add white Gaussian noise with PSD equal to -168 dBm/Hz. Thus, the signal to noise ratio (SNR), without path loss and fading, on each sub-channel is 115 dB. The baseline systems use an OH of 0.8 μs that corresponds to the value of CP employed in the IEEE 802.11 standard [12].

Fig. 1 shows the capacity (5) as a function of the OH duration for both OFDM and FMT for 100 class B channel realizations. The distance between transmitter and receiver equals 10 m. As we can see in both cases an optimal OH that maximizes the capacity (5) can be found for each channel realization. Furthermore, we can see that in general the capacity is not a convex function of the OH, this is especially true for FMT, but in general it can also happen for OFDM. This observation justifies the exhaustive search (7) over the values of OH to find the optimal OH value to be used for each channel realization. On the other hand, we can see that the capacity curves are relatively flat around the optimal OH value. Therefore, the choice of an OH close to the optimal one will not dramatically change the capacity value w.r.t. the maximum. These observations justify our proposal to design the OH according to the capacity-optimal OH CDF as described in Section 3.2. From Fig. 1 we can also notice that the OH adaptation significantly improves the system performance w.r.t. the baseline system that deploys an OH of 0.8 μs.

Figs. 2,3 respectively show the capacity-optimal OH CDFs for FMT and for OFDM for each channel class and for different distances between transmitter and receiver. From Fig. 2 (see the first 5 sub-plots starting from the top), we can see that for FMT the optimal OH CDF does not appreciably depend on the experienced channel class but it shows a strong dependance on the distance

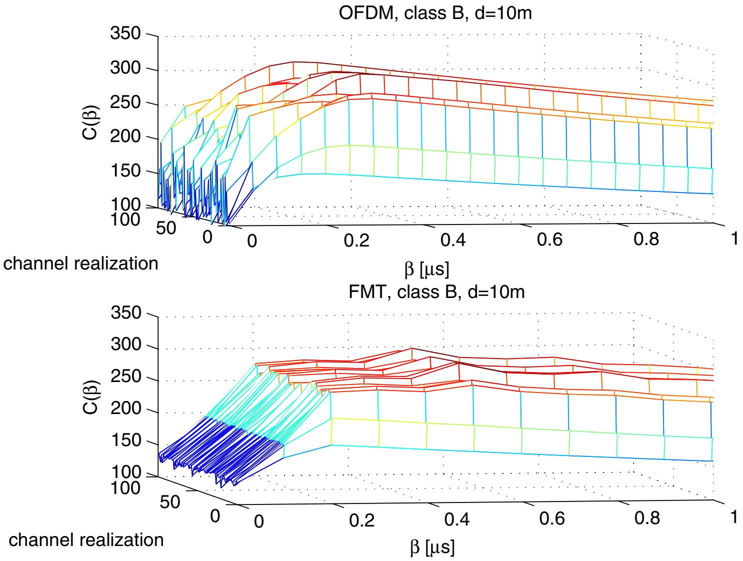


Fig. 1. Capacity as a function of the OH duration for 100 class B channel realizations using OFDM (top), and FMT (bottom). The distance between transmitter and receiver is set equal to 10 m.

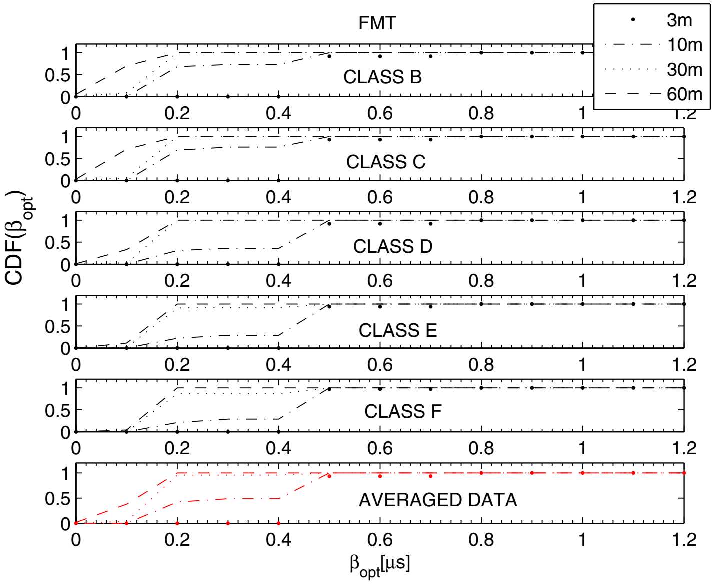


Fig. 2. Optimal OH CDF for FMT considering each single channel class, and all the classes together. The distances between transmitter and receiver are set equal to 3 *m*, 10 *m*, 30 *m*, and 60 *m*.

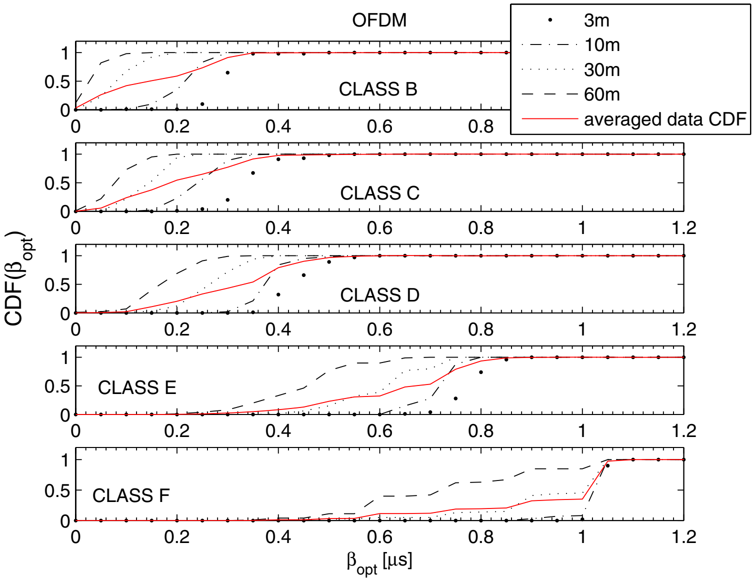


Fig. 3. Optimal CP CDF for OFDM considering channels of class B, C, D, E, and F. The distances between transmitter and receiver are set equal to 3 *m*, 10 *m*, 30 *m*, and 60 *m*.

between transmitter and receiver. Thus, as explained in Section 3.2 for each value of distance considered, we choose a near optimal OH value as such value that renders the optimal OH CDF equal to 0.99(obtained averaging the data across all the channel classes, see the last sub-plot of Fig. 2). The corresponding set of OH values is $\mathbb{P}_{FMT} = \{\beta_{3,FMT}^{(99\%)} = 0.8\mu s$, $\beta_{10,FMT}^{(99\%)} = 0.5\mu s$, $\beta_{30,FMT}^{(99\%)} = 0.2\mu s$, $\beta_{60,FMT}^{(99\%)} = 0.2\mu s\}$.

Regarding Fig. 3, we can see that for OFDM the optimal OH CDF depends more on the channel class than on the distance. Thus, as assumed in [4], for each channel class, we choose a near optimal value of OH (or equally CP) that renders the optimal OH CDF (obtained averaging the data over the distances) equal to 0.99. The corresponding set of OH values is $\mathbb{P}_{OFDM} = \{\beta_{B,OFDM}^{(99\%)} = 0.4\mu s$, $\beta_{C,OFDM}^{(99\%)} = 0.5\mu s$, $\beta_{D,OFDM}^{(99\%)} = 0.6\mu s$, $\beta_{E,OFDM}^{(99\%)} = 0.9\mu s$, $\beta_{F,OFDM}^{(99\%)} = 1.1\mu s\}$. It is worth noting that the application to FMT of the criterion used to compute the limited set $\mathbb{P}_{OFDM}$ for OFDM, would return a single value of OH equal to 0.8 μs. This is because, as shown in Fig. 2, the optimal OH of FMT does not depend on the channel class. Thus, for all the channel classes we would obtain the same value of β that renders all the CDFs equal to 0.99. This criterion could be adopted to design a globally acceptable value of OH for FMT.

The different behavior of the optimal OH CDFs for FMT and OFDM is due to the use of different sub-channel pulses and equalization scheme. In FMT the ICI is minimized via the design of the OH factor together with the sub-channel pulse, while the ISI is mitigated with the use of the sub-channel equalizer. In OFDM since we deploy a single tap equalizer, the OH (cyclic prefix) has to be designed such that we tradeoff between ISI+ICI and noise. Indeed, multichannel equalization is in principle applicable in OFDM in order to mitigate the ICI with a CP shorter than the channel response, which however, increases significantly complexity.

Let us now focus on the optimal OH CDF of OFDM (see Fig. 3). As previously observed, the optimal OH depends on the experienced channel class. This is because each channel class is characterized by a certain r.m.s. delay spread, and as it is well known, in OFDM the channel temporal dispersion that causes ISI is handled with the CP. Consequently, for each channel class a different value of OH (or equally CP) is needed to deal with the ISI term. Obviously, the for the ICI term considerations similar to the ones done for FMT are also valid for OFDM. Now, in Fig. 4 we report the complementary CDF (CCDF) of the capacity (5) obtained for FMT and OFDM with both the optimal OH value (7) and the sub-optimal ones above listed. The used channel classes are the B, D, and F. The distance between transmitter and receiver is set equal to 3 m, 10 m and 30 m. As we can see, in almost all the cases, FMT with OH optimized outperforms OFDM with OH optimized. This is true using either the optimal OH adaptation (7) based on the exhaustive search, or the simplified OH adaptation based on the limited search over the sets $\mathbb{P}_{OFDM}$ and $\mathbb{P}_{FMT}$. Note that, also if not shown for space limitation, the CCDF of the capacity for OFDM and FMT with OH equal to 0.8 μs would give worse performance than the showed one. As for instance see the CCDF of the baseline OFDM system in [4].

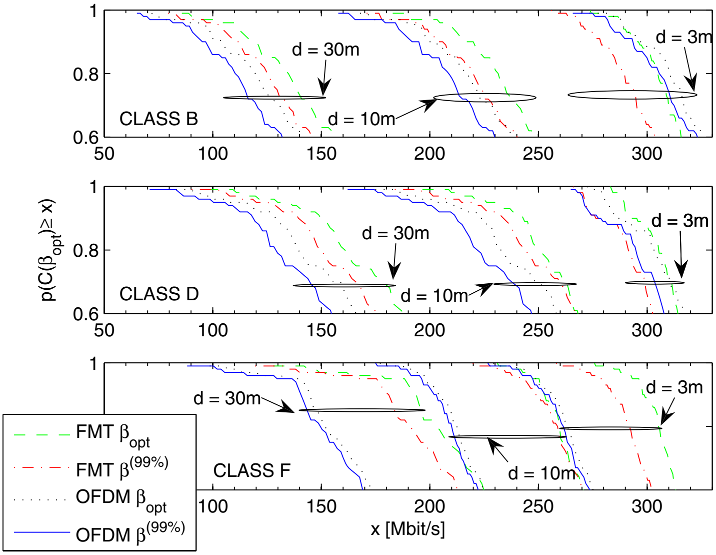


Fig. 4. CCDF of capacity using OFDM and FMT with optimal and limited OH adaptation. The used channel classes are the B,D, and F. The distances between the transmitter and the receiver are set equal to 3 m, 10 m, and 30 m.

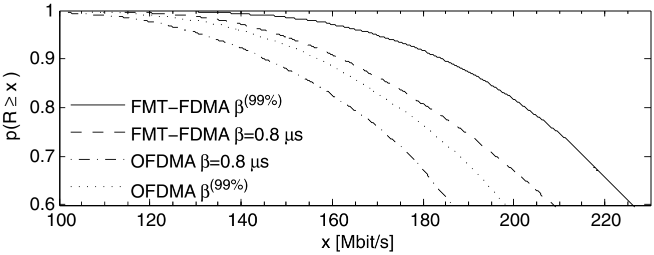


Fig. 5. CCDF of the aggregate network rate obtained using the limited OH adaptation for both OFDMA and FMT-FDMA. Also plotted are the CCDFs obtained using FMT-FDMA and OFDMA with a fixed OH of 0.8 μs.

Finally, in Fig. 5 we show the CCDF of the aggregate network rate obtained using the algorithm exposed in Section 4 for both FMT-FDMA and OFDMA. Also shown are the CCDF obtained using the baseline systems that deploy an OH equal to 0.8 μs. The network is composed by 4 users. The weights $p^{(u)}$ are equal to 0.25. Therefore, we have considered a proportional fair resource allocation. The users experience channels belonging to the same class, the channel class is randomly selected, and the distance between each user and the AP is drawn randomly between 3 m and 60 m. As we can see, the limited OH adaptation to the channel condition improves the performances of both FMT-FDMA and

OFDMA w.r.t. the baseline system that deploys an OH equal to 0.8 μs. More precisely, with probability equal to 0.9, the limited OH adaptation respectively improves the aggregate network rate of about 7% for OFDMA, and of about 12% for FMT-FDMA. From Fig. 5, we also notice that the use of adaptive FMT-FDMA, with probability equal to 0.9, improves the aggregate network rate of about 27% w.r.t. the use of OFDMA with a fixed CP value equal to $0.8\mu s$.

6 Conclusions

The use of adaptive FMT could further improve the WLAN standard capacity w.r.t. the use of adaptive OFDM. This is true for both the single user case and the multi user case that deploys FDMA. Ongoing work is assessing the complexity implications and the approaches to reduce it.

References

1. Kalet, I.: The Multitone Channel. IEEE Trans. Commun. 37(2), 119–124 (1989)
2. Tonello, A.M., Pecile, F.: Analytical Results about the Robustness of FMT Modulation with Several Prototype Pulses in Time-Frequency Selective Fading Channels. IEEE Trans. on Wireless Commun. 7(5), 1634–1645 (2008)
3. Seoane, J., Wilson, S., Gelfand, S.: Analysis of Intertone and Interblock Interference in OFDM when the Length of the Cyclic Prefix is Shorter than the Length of the Impulse Response of the Channel. In: Proc. of IEEE GLOBECOM, Phoenix, AZ, USA, pp. 32–36 (1997)
4. D'Alessandro, S., Tonello, A.M., Lampe, L.: Improving WLAN Capacity via OFDMA and Cyclic Prefix Adaptation. In: IEEE IFIP Wireless Days, Paris, France (2009)
5. Ercegl, V., Shumacher, L., et al.: IEEE P802.11 Wireless LANs, TGn Channel Models, doc.: IEEE 802.11-03/940r4 (2004)
6. Pecile, F., Tonello, A.M.: On the Design of Filter Bank Systems in Power Line Channels Based on Achievable Rate. In: Proc. of IEEE Int. Sym. on Power Line Communications and its Applications 2009, Dresden, Germany (2009)
7. Cherubini, G., Eleftheriou, E., Olcer, S.: Filtered Multitone Modulation for Very High-Speed Digital Subscriber Lines. IEEE J. Sel. Areas Commun. 20(5), 1016–1028 (2002)
8. Tonello, A.M.: Asynchronous Multicarrier Multiple Access: Optimal and Sub-Optimal Detection and Decoding. Bell Labs Tech. Journal, special issue: Wireless Radio Access Networks 7(3), 191–217 (2003)
9. Tonello, A.M., Pecile, F.: Efficient architectures for multiuser FMT systems and application to power line communications. IEEE Trans. on Commun. 57(5), 1275–1279 (2009)
10. Proakis, J.: Digital Communications, ch. 10, 4th edn. Mc Graw Hill, New York
11. Tonello, A.M., D'Alessandro, S., Lampe, L.: Bit, Tone and Cyclic Prefix Allocation in OFDM with Application to In-Home PLC. In: Proc. of IEEE IFIP Wireless Days 2008, Dubai, United Emirates, pp. 1–5 (2008)
12. IEEE Std.802.11: Wireless LAN Medium Access Control and Physical Layer Specification (2007)
13. Luenberger, D.G.: Linear and Nonlinear Programming. Addison-Wesley, Reading (1984)

Challenges in Gbps Wireless Optical Transmission

Mike Wolf[1], Jianhui Li[1], Liane Grobe[1], Dominic O'Brien[2],
Hoa Le Minh[2], and Olivier Bouchet[3,⋆]

[1] Communications Research Laboratory, Ilmenau University of Technology, P.O. Box 100565,
D-98684 Ilmenau, Germany
[2] Department of Engineering Science, University of Oxford, Parks Road Oxford, OX 13PJ, UK
[3] France Telecom, Orange Labs, 4 rue Clos Courtel, 35512 Cesson-Sevigne, France

Abstract. In this paper, the link budget of Gbps wireless infrared indoor communication is analysed. We particularly focus on the receiver sensitivity and identify the most suitable wavelengths range. We show that an optical receiver operating at 1 Gbps will hardly achieve the shot noise limit, which is determined by the received amount of background light. Regarding the link budget, we present two case studies. One deals with (very) short range communication, the other one with a wireless personal area network. We reveal that a network demands for avalanche photodiodes as well as beam steering. This clearly causes major challenges regarding compact and inexpensive components.

Keywords: infrared, communication, eye safety, photodetector, link budget, receiver sensitivity, angle diversity, imaging receiver, non-imaging receiver.

1 Introduction

As a part of the EU Seventh Framework R&D programme (FP7), the hOME Gigabit Access (OMEGA) project aims at bridging the gap between mobile broadband terminals and the wired backbone at home. To provide Gbps connectivity, three main technologies — RF, power line and infrared (IR) — are considered. This paper focuses on IR transmission.

IR radiation exhibits a number of characteristics which qualify it as an appropriate alternative to RF for short range indoor transmission. First of all, IR takes advantage of a completely unregulated and unlicensed spectral range. Since IR radiation does not travel through walls, systems operating in separate rooms do not interfere with each other. For the same reason, the optical medium promises high security against eavesdropping. Furthermore, an IR transmitter does not produce any "electrosmog" in the ideal case.

However, besides these advantages it is known that IR transmission is associated with some real challenges. The most important one is definitely the limited receiver sensitivity. Typically (and even at 1 Gbps), a RF receiver will outperform its IR-counterpart by several tens of decibels. The enormous difference is by far not only a result of detecting the signal coherently or non-coherently. It is a result of the completely different physical mechanisms which underlie the detection [1].

[⋆] This work is supported by the European Union Seventh Framework Programme referred as OMEGA [www.ict-omega.eu].

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 484–495, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

For free space optical links (such as those between satellites or between buildings), the limited receiver sensitivity will be (more than) compensated by a very small path loss, since highly directive transmitters and receivers are used. In this case, the link budget profits from the fact that optical radiation can be focused very well leading to huge "antenna gains".

However, optical indoor communication considered here demands for a reasonable coverage. Even if line-of-sight (LOS) is assumed, it is thus not as straightforward to benefit from a directional gain. To ensure coverage, beam steering needs to be applied. Currently and in the near future, two concepts are realistic and applicable at both the transmitter and the receiver. One uses a mechanical steering of a narrow beam [2]. The other one is based on angle diversity [3], i.e., the solid angle to be covered is divided into a number of sub-sectors, where each sub-sector corresponds to a different transmit/receive angle. In this case, the beam steering is discrete — comparable to switched beam antennas. Two angle diversity approaches can be used. In one case, each laser or photodiode is equipped with its own (possibly non-imaging) optics. These "directional optics" are accordingly aligned, where a certain overlapping is required. In the other case, an array of lasers or photodiodes is combined with an imaging optics — very similar to the sensor-lens combination used in digital cameras.

In this paper, the link budget for non-return-to-zero (NRZ) On-Off Keying (OOK) LOS transmission at a data rate of 1 Gbps is analysed. We will particularly focus on the receiver sensitivity (section 3). It will be shown that silicon photodiodes offer a better receiver sensitivity than photodiodes made of InGaAs or other ternary semiconductors. The primary reason for that is the photodiode capacitance, which is desired to be as small as possible. We will show that the detector will not reach the shot noise limit (determined by the amount of received background light), which makes a good link budget even more challenging. Two case studies presented in section 4 will point out clearly that an optical wireless personal area network (operating at 1 Gbps) demands for beam steering concepts offering large directional gains. This makes the design of compact and lightweight components not easy.

2 Eye Safety

The transmit power is an important link budget parameter. It is ultimatively limited by laser safety constraints. Laser safety is covered by the international standard IEC 60825-1. It is important to note that a new edition of this standard, designated 60825-1:2007 edition 2, has recently been published [4]. In this edition, the measurement condition for diverging sources has been relaxed. The following focuses on the new eye safety constraints.

The classification of any diverging source (with a half-intensity angle larger than a few degrees) can be referred to its on-axis radiant intensity I_0 (in mW/sr). I_0 scaled by 4π (the solid angle of a sphere) is nothing else but the "equivalent isotropic radiated power" (EIRP) which is commonly used for RF link budget analysis. By using I_0, the class 1 limit — "safe under all foreseeable conditions" [4] — to be used here depends only on the apparent source diameter D and on the wavelength λ.

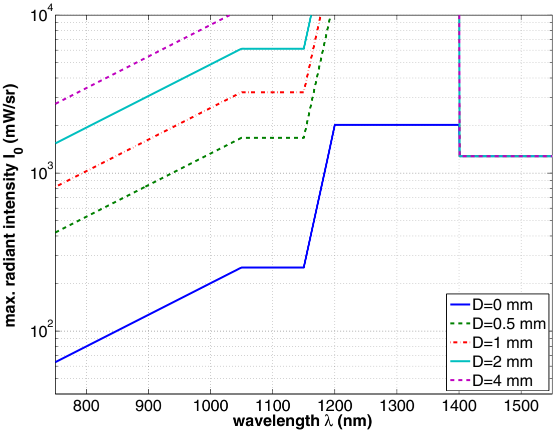


Fig. 1. Permitted on-axis radiant intensity for class 1 sources depending on the source diameter D

The I_0 limits according to edition 2 are shown in Fig. 1. For $\lambda > 1200$ nm, the permitted I_0 can exceed 1000 mW/sr, even for a point source, i.e., $D = 0$ mm. This is in fact a very large value — 1000 mW/sr corresponds to an optical EIRP of 12 W. For $\lambda > 1200$ nm the eye safety will most likely not cause any problem with respect to the system design. Unfortunately, such wavelengths are outside the detection range of inexpensive silicon photodiodes.

At 800 nm, where fast silicon detectors are available (see next section), I_0 is limited to about 80 mW/sr corresponding to an EIRP of 1 W. This is many times more than permitted compared to previous standard editions, but larger values may be still desirable. Especially, if the transmitter shall profit from a large directional gain, an additional diffuser[1] needs to be applied to increase the apparent source size D. Fig. 1 shows that a diffuser diameter of $D = 1$ mm is theoretically sufficient in order to increase I_0 to 1000 mW/sr. Anyway, if each laser of a laser diode array (used for a transmit beam steering) needs to be equipped individually with a diffuser, much technological effort has to be paid to produce compact and lightweight equipment.

3 Receiver Sensitivity — The Major Problem

The receiver sensitivity has a significant impact on the residual system design. Regarding the preamplifier, transimpedance or bootstrap-transimpedance designs are used to obtain a good noise performance altogether with a sufficient bandwidth and a good dynamic range. The noise and sensitivity modelling described in section 3.2 is independent on the preamp design, but the concrete values for the parameters must be assigned very carefully. The photodiode capacitance C_D as one very important parameter depends

---

[1] For $D > 0$, it is assumed that the apparent location of the source corresponds to the physical location of the diffuser.

not only on the photodiode area but also on the photodiode material itself. Inexpensive silicon, which promises a much lower capacitance than InGaAs or other ternary or quaternary semiconductors, can only be used in the 800 nm range but not at 1200 nm and above. This topic will be addressed in section 3.3.

In the opposite to RF receivers, which may be interference limited, IR detectors are generally noise limited. At 1 Gbps, the noise exhibits also a strong f^2 component, i.e., a component whose power spectral density increases with f^2. This makes the design of a power efficient system even more challenging than at lower data rates and bandwidths, respectively. It will be shown that — more expensive — avalanche photodiodes (APDs) are unavoidable in many cases.

3.1 Choosing the Right Modulation Scheme

The receiver sensitivity depends, via the required signal-to-noise ratio, on the modulation scheme as well. The most popular intensity modulation schemes for wireless IR transmission are by far OOK and PPM (Pulse-Position Modulation). Both schemes exhibit only two signal levels making the laser diode driver much easier to build and much more power efficient than a linear driver required for subcarrier modulations or pulse amplitude modulation. The popularity of PPM has primarily two reasons. Firstly, compared to uncoded OOK, it may provide an advantage from the required average optical power point of view. Secondly, PPM has a favourable spectral characteristic, cf. [5].

However, compared to OOK both advantages of PPM are at the expense of an increased bandwidth. This is a serious issue for Gbps transmission, since the speed of the devices is limited, cf. section 3.3. Furthermore, the power advantage of PPM will turn out to be a loss, if the receiver sensitivity is limited primarily by f^2 noise, whose variance increases with the third power of the bandwidth [5,6].

In conclusion, (NRZ) OOK can be seen as a good choice for Gbps operation, although it needs to be combined with a line coding scheme[2] to ensure an appropriate spectral characteristic and DC balance [6,7]. With respect to the following analysis, 8B10B line coding is assumed, which increases the bit rate at the modulator input to 1.25 Gbps. Forward error correction is not considered here. Nevertheless, our analysis reveal that a low redundancy (7%) Reed-Solomon code as used for fiber optics [8] promises an optical 3 dB gain, even if f^2 noise dominates.

3.2 Noise and Sensitivity Modelling

The bit error rate p_b for NRZ-OOK can be expressed as

$$p_\mathrm{b} = \frac{1}{2} \cdot \mathrm{erfc}\sqrt{\frac{\varrho}{2}} \quad \text{with} \quad \varrho = \frac{(d_\mathrm{eucl}/2)^2}{\sigma_n^2},$$

where d_eucl is the eye-opening at the sampling time (assuming no noise) and σ_n^2 is the noise variance. For NRZ-OOK with an average optical receive power P_rx (the peak power is $2P_\mathrm{rx}$), d_eucl is given as

$$d_\mathrm{eucl} = 2P_\mathrm{rx}R_\lambda M,$$

---

[2] PPM can be regarded as a line coding scheme combined with OOK.

if the receive filter ensures a maximum eye-opening. This leads to

$$\varrho = \frac{(P_{\mathrm{rx}} R_{\lambda} M)^2}{\sigma_n^2}.$$

Assuming a BJT-based input stage, the noise variance σ_n^2 is given as [9]

$$\sigma_n^2 = \underbrace{\left(\underbrace{2q(P_{\mathrm{bg}} + 2P_{\mathrm{rx}}) R_{\lambda} M^{2+x_{\mathrm{APD}}}}_{\text{shot noise}} + \underbrace{2qI_{\mathrm{b}} + \frac{4k_B T}{R_L}}_{\text{preamp white noise}} \right) I_2 R_{\mathrm{b}} +}_{\text{white noise}}$$

$$\underbrace{\left(\frac{2qI_{\mathrm{c}}(2\pi C_{\mathrm{tot}})^2}{S^2} + 4k_B T(R_{\mathrm{bb}} + R_{\mathrm{s}})(2\pi C_{\mathrm{D}})^2 \right) I_3 R_{\mathrm{b}}^3}_{\text{preamp } f^2 \text{ noise}} . \qquad (1)$$

Table 1 of the Appendix summarizes the symbol definitions and the parameters used for the analysis. With respect to the electrical receive filter, a 5th order Bessel filter with a 3 dB cut-off frequency of $R_{\mathrm{b}}/2$ is assumed. This filter leads to an eye-opening penalty of 0.5 dB[3], which is additionally considered with respect to d_{eucl}. The preamp's first transistor is assumed to be a state of the art silicon germanium transistor (such as Infineon BFP650) with a very low base spreading resistance. In the following, the photodiode parameters, which have a major impact on the sensitivity, are discussed.

3.3 Photodiode Capacitance and Responsivity

Wireless optical transmission is currently feasible at wavelengths between about 400 nm and 2000 nm. Two candidate bands are of special interest. One at about 800 nm, where Si-based photodiodes can be used. The other one is between about 1300 nm and 1550 nm, where components are readily available from fiber optics. The wavelength determines 3 major parameters contained in Eq. (1): the photodiode responsivity R_{λ}, the photodiode capacitance C_{D} and the optical power P_{bg} of the received background light. Thus, the wavelength needs to be selected very carefully in order to obtain a satisfactory link budget.

Photodiodes used for Gbps optical indoor transmission need to offer not only a short rise time. They should also exhibit a large area A_{D}, a sufficiently large R_{λ} as well as a low C_{D}. Unfortunately, all these properties can not be ensured at the same time.

For a given thickness d_i of the i-region, the capacitance of a PIN-photodiode (or APD) can be estimated to

$$C_{\mathrm{D}} = \frac{\varepsilon_0 \varepsilon_r}{d_i} \cdot A_{\mathrm{D}},$$

where ε_r is the relative permittivity of the semiconductor material. Thus, from the capacitance point of view (and also from the R_{λ} point of view), a large d_i is desirable. However, since the transit time of the carriers increases with d_i as well, the rise time requirements put an upper limit to d_i.

---

[3] For this filter type, a 3 dB cut-off frequency of $R_{\mathrm{b}}/2$ ensures a good trade-off between the (vertical) eye-opening penalty, the noise power and the data dependent jitter.

Silicon Photodiodes available on the market exhibit a wide variety of spectral characteristics, which mainly depend on the chosen d_i and on the semiconductor process, respectively.

Basic rise time estimations for Si photodiodes show that $d_i = 20\ \mu$m can be seen as a realistic value for Gbps OOK operation: If a reverse voltage of 40 V is assumed, which gives an electrical field of 2 V/μm, the velocity of the (slower) holes is 50 μm/ns [10]. This means that the impulse response is as fast as 0.4 ns.

For a Si PIN-photodiode with $d_i = 20\ \mu$m, the capacitance per area is about 5 pF/mm^2. The thickness determines also the quantum efficiency η and thereby the responsivity R_λ, which is given by

$$R_\lambda = \eta \frac{\lambda}{1.24\ \mu\mathrm{m}} \mathrm{A/W}.$$

For $d_i = 20\ \mu$m and a wavelength of 800 nm, the quantum efficiency (ignoring any reflection losses or carrier recombinations) is still about 0.8, see [11], which gives $R_\lambda = 0.5$ A/W.

InGaAs Photodiodes devices are usually epitaxially grown and it is very difficult to grow devices with the thickness of i-regions available in silicon. Work in [12] details the growth of devices with 5 μm i-regions corresponding to a capacitance of 23.5 pF/mm^2, but these have high leakage. Further optimization work was undertaken with limited success which shows the challenge of fabricating these detectors. Assuming devices with 23.5 pF/mm^2 compared with 5 pF/mm^2 for silicon, there is already an area reduction of a factor 5. “Typical” InGaAs devices are not as good as this, and can easily have capacitances of 60 pF/mm^2, which is 12 times the value of Si devices available on the market.

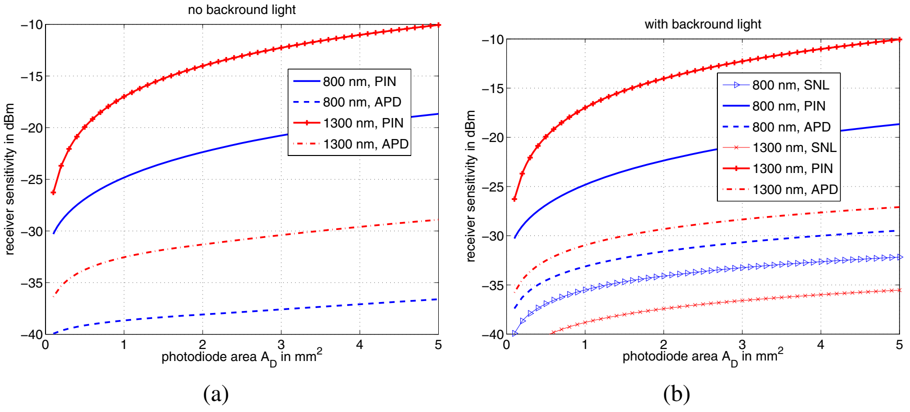
Similar conclusions can be made for Ge. Although state of the art Germanium on Silicon (Si is used for the substrate) photodiodes provide excellent properties for fiber optic applications, the usage for indoor applications is again restricted by very thin i-layers between only 1 μm to 5 μm.

InGaAs is a direct semiconductor with a sharp edge at the cut-off wavelength. Thus at 1.3 μm, nearly 100% of the photons will be absorbed suggesting $R_{1.3\mu\mathrm{m}} \approx 1$ A/W which is twice as large as $R_{850\mathrm{nm}}$. However, typical values range from about 0.6 A/W to 0.9 A/W [13].

3.4 Received Ambient Light

If ambient light is detected additionally, shot noise will be superimposed to the signal current. The amount of noise depends directly on the optical DC-power P_{bg} of the received ambient light, see Eq. (1). Measurements in [14] prove that sun light, which can be seen as the strongest source for P_{bg}, can be well modelled as a thermal radiator operating at a temperature of 5500 K. According to this model, the background light radiance decreases with increasing wavelengths (for $\lambda > 500$ nm). If the radiance at $\lambda = 800$ nm acts as a reference, the radiance is decreased by a factor 3 for $\lambda = 1300$ nm and a factor 5 for $\lambda = 1550$ nm, respectively.

With respect to wireless IR transmission, the background light induced shot noise is often assumed to be the dominating noise source. This may lead to the premature



(a) (b)

Fig. 2. Receiver sensitivity without (a) and with (b) incorporated background light. Fig. 2(b) shows additionally the shot noise limit "SNL" (only background light induced shot noise).

conclusion that systems operating at 1300 nm and above profit from a better receiver sensitivity. In section 3.6 we show that this is not the case for 1 Gbps transmission.

3.5 Receiver Sensitivity Estimation — No Ambient Light Incorporated

Fig. 2(a) shows the receiver sensitivity, if the photocurrent does not include a background light induced shot noise component, i.e., $P_{\mathrm{bg}} = 0$. It can be seen that APD based receivers outperform their PIN-photodiode based counterparts by about 15 dB. An InGaAs receiver operating at 1300 nm — this wavelength is chosen as a representative for the considered second band — does not achieve the sensitivity of the corresponding Si device operating at 800 nm. At a photodiode area of 0.5 mm^2, the gap between Si and InGaAs is about 5 dB for APDs and 7.5 dB for PIN-photodiodes, see Fig. 2(a).

Clearly, RF receivers will offer a much better sensitivity. Even if optical receivers would operate at the corresponding quantum noise limits (10 photons per bit), the sensitivities would be "only" -55 dBm at 800 nm and -57 dBm at 1300 nm, respectively. These values show clearly how challenging it is to provide coverage (in a sense of a wireless personal area network). For RF receivers operating at the same data rate, -70 dBm is surely not unrealistic.

3.6 Receiver Sensitivity Estimation — Ambient Light Incorporated

The ambient light is assumed to be fully diffuse, i.e., its spectral radiance $L_{\lambda,\mathrm{bg}}$ is independent of the rotation of the receiver. In this case, for a given detector area A_{rx} and a given (sub-sector) receiver FOV Ψ_{rx} (half-cone angle), the received amount of background light (per sub-sector) is [11]

$$P_{\mathrm{bg}} = L_{\lambda,\mathrm{bg}} \Delta\lambda A_{\mathrm{rx}} \sin^2(\Psi_{\mathrm{rx}})\,\pi. \tag{2}$$

In Eq. (2), it is assumed that $L_{\lambda,\mathrm{bg}}$ is constant within the transmission band of the optical filter with bandwidth $\Delta\lambda$. A_{rx} is not the photodiode area — it is the effective detection area, which is increased from A_{D} to A_{rx} by means of an (imaging or non-imaging) optical concentrator. The following analysis assume an ideal optical concentrator with a "directional gain" G of

$$G = \frac{A_{\mathrm{rx}}}{A_{\mathrm{D}}} = \frac{n_c^2}{\sin^2(\Psi_{\mathrm{rx}})}.$$

In this case, the amount of received background light is independent on the FOV, since the product of the effective detection area and the solid angle is a constant.

Fig. 2(b) shows the receiver sensitivity, when background light with a spectral radiance $L_{\lambda,\mathrm{bg}} = 0.04$ μW/(mm^2·sr·nm) @ 800 nm is considered[4]. In the case of PIN-photodiodes, no difference can be observed between Fig. 2(a) and Fig. 2(b), since the variance of f^2 noise exceeds the variance of the ambient light induced shot noise by several magnitudes. To demonstrate this, the shot noise limits are also shown[5]. This motivates the usage of APDs, which increase the signal current by a factor M. It can be observed from Fig. 2(b), that APDs indeed outperform PIN-photodiodes, although the shot noise variance increases disproportionately by $M^{2+x_{\mathrm{APD}}}$, where x_{APD} is the excess noise factor. For $A_{\mathrm{D}} = 1$ mm^2, the gap between APDs and PIN-photodiodes is 7.5 dB at 800 nm and 15 dB at 1300 nm.

4 Required Radiant Intensity

Assuming perfect on-axis alignment and a LOS channel, the received signal power is given by

$$P_{\mathrm{rx}} = \frac{I_0}{d_{\mathrm{tx,rx}}^2} \cdot A_{\mathrm{rx}}.$$

Since I_0 multiplied with 4π corresponds to the EIRP of the transmitter, the quotient $I_0/d_{\mathrm{tx,rx}}^2$ is directly the (on-axis) optical irradiance at the receiver.

Fig. 3 shows the required radiant intensity for a 1 m reference distance[6]. Perfect alignment (on-axis operation) is assumed and no link margin is incorporated. As a result of the limited sensitivity offered by PIN-photodiodes, only APDs with 4 different areas A_{D} are considered. As opposed to Fig. 3(a), the influence of ambient light is taken into account for Fig. 3(b). The required I_0 is shown as a function of the (sub-sector) receiver FOV, where an ideal optical concentrator is assumed to be used. The following presents two case studies.

4.1 Case Study I

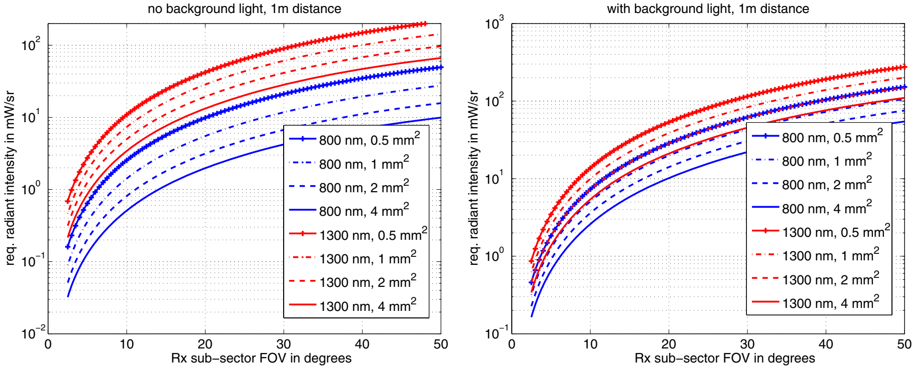
The first scenario could be treated as a cable replacement between a laptop and a hand-held device, where only a very short distance of 25 cm is assumed. The system FOV is assumed to be 20° and the operation wavelength to be 800 nm. If neither the transmitter nor the receiver uses beam steering, the sub-sector FOV equals the system FOV.

---

[4] In [15], this value of $L_{\lambda,\mathrm{bg}}$ is denoted as "typical" for bright skylight and $\lambda = 850$ nm.

[5] In this case, the noise variance is reduced to the term $2qP_{\mathrm{bg}}R_{\lambda}M^2$.

[6] If the distance $d_{\mathrm{tx,rx}}$ is changed by a factor k, I_0 changes by a factor k^2.



(a) (b)

Fig. 3. Required on-axis radiant intensity without (a) and with (b) incorporated background light for a reference distance of 1 m (ideal optical concentrator, no margin)

Assuming an APD area of 1 mm^2, the required radiant intensity for on-axis operation in bright skylight is (20 mW/sr)/$4^2 = 1.25$ mW/sr. Operation at the half-intensity angles increases the required I_0 by a factor 4. If a further 5 dB margin is considered (penalties will surely occur due to a non-ideal concentrator, losses in the optical filter, etc.), the required I_0 needs to be further increased to about 16 mW/sr.

According to Fig. 1, for this value no additional diffuser is required from the eye safety point of view. (If a PIN-photodiode shall be used instead of an APD, the required power increases roughly by 7.5 dB, which gives an I_0 above the point source limit.)

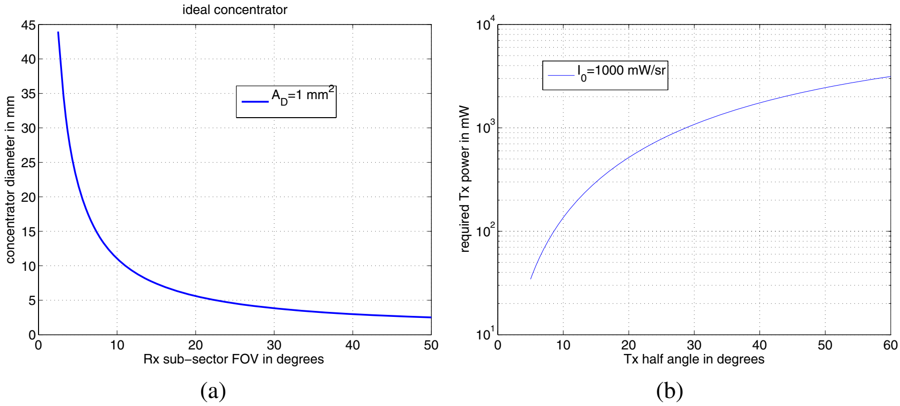
For Fig. 3(b), it is assumed that an ideal concentrator is used. Fig. 4(a) shows that the corresponding diameter of the concentrator aperture is about 6 mm. Assuming an Lambertian transmit characteristic, the total transmit power would be about 8 mW, cf. Fig. 4(b). All these values are really convincing.

4.2 Case Study II

The second example shall be a wireless personal area network with a ceiling mounted base station (BS). The BS and the terminals are assumed to have a system FOV of 45° (half-cone angle). Assuming that the BS is located 3 m above the terminals, the BS defines a cell with a 3 m radius in the horizontal plane of the terminals. The maximum LOS distance $d_{\mathrm{tx,rx}}$ within the cell is therefore $\sqrt{2} \cdot 3$ m.

If both the transmitters and the (opposite) receivers would not use beam steering, the transmission would strongly suffer from multipath dispersion. Therefore, we assume that beam steering is used at least at the receive site. The sub-sector FOV shall be (exemplarily) reduced to 10°.

Supposing again an APD area of 1 mm^2, the required on-axis radiant intensity for $d_{\mathrm{tx,rx}} = \sqrt{2} \cdot 3$ m would be about (5 mW/sr) $\cdot\, 2 \cdot 9 = 90$ mW/sr, cf. Fig. 3(b). If operation at the half-intensity angle altogether with a 5 dB margin is postulated again, the required I_0 will be about 1150 mW/sr. For eye safety reasons, the transmit laser now



(a) (b)

Fig. 4. (a) Detector diameter for $A_\mathrm{D} = 1\ \mathrm{mm}^2$ depending on the Rx sub-sector FOV. (b) Required Tx power for $I_0 = 1000$ mW/sr depending on the half-power angle of a Lambertian transmitter.

needs to be equipped with a diffuser. If the transmitter uses only one single transmit element with a system FOV of 45°, the total optical transmit power would be about 2.3 W, see Fig. 4(b). At least for battery powered terminals this value is not acceptable. Therefore, the transmitter has to use beam steering additionally, or the sub-sector FOV of the receiver has to be further reduced.

For a sub-sector FOV of 10°, the diameter of the input aperture of the optics will be at least 11 mm, cf. Fig. 4(a). Supposing an angle diversity concept (and not a mechanical tracking), the diversity order needs to be about 20-25 — depending on the overlapping between the individual beams. This number shows clearly that not each of the 20-25 APDs can be equipped with its own concentrator (each having an 11 mm diameter). The result would be absurdly bulky and heavy. An imaging receiver concept, where an APD array is equipped with a lens, is much more preferable. However, even this receiver is very challenging, since the (wide angle) lens needs to be inexpensive, compact and lightweight. Here solutions similar to the one used in mobile-phone cameras are required. Furthermore, the APD array with a total area of 20-25 mm^2 is surely more expensive than a single 1 mm^2 APD discussed in the previous example. Angle diversity concepts based on imaging optics are also possible at the transmitter, but require the usage of vertical-cavity surface-emitting lasers.

4.3 Demonstrator

Within the OMEGA project, a 1 Gbps IR demonstrator was successfully built. Angle diversity with a diversity order of 3 is used at both the transmitter and the receiver, where the sub-sector half-intensity angles are 5°. The 825 nm transmitter consists of 3 differently aligned lasers, each equipped with a holographic diffuser. The receiver uses 3 differently aligned 0.2 mm^2 silicon APDs, each equipped with a lens offering a gain of 130 (linear scale). Without ambient light, a sensitivity of -35 dBm was achieved. The demonstration clearly shows the possibility of optical indoor transmission at 1 Gbps.

However, it emphasizes also that a compact and lightweight angle diversity concept, which provides a large system FOV as required for networks, is really challenging and rather impossible to built, if only commercial optical and opto-electronical components are used.

5 Conclusion

At 1 Gbps, it is very difficult to achieve a satisfying receiver sensitivity. The main reason is f^2 noise, whose variance increases with the third power of the bandwidth and the second power of the photodiode capacitance. InGaAs photodiodes exhibit a much larger capacitance than well designed silicon photodiodes. Thus at 1 Gbps, the wavelengths range at about 800 nm is still a good choice. By means of two case studies it was shown that a (silicon) PIN-photodiode may be an option — but only for very short distances in the cm-range. For wireless personal area network applications, which demand for coverage, APDs need to be applied. Unfortunately, they are not only more expensive than PIN-photodiodes but also require a high reverse voltage (more than 100 V), which could be disadvantageously from the chip-integration point of view. Wireless optical networks operating at 1 Gbps demand also for beam steering — not only to mitigate multipath dispersion. With the receiver sensitivity in mind (which does not reach the shot noise limit), it is also required to reduce the path loss notably. From the power consumption point of view, beam steering preferably takes place at both the receive and the transmit site. Since the diversity order of angle diversity concepts needs to be large (20-25 in case study II), it is impossible to equip each photodiode with its own optics. The resulting components would be bulky and heavy. Thus APD arrays need to be combined with low cost, compact and lightweight optics as known from mobile phones with digital cameras. Imaging optics known as "Gabor superlenses" could be an interesting option.

References

1. Wolf, M., Kress, D.: Short-Range Wireless Infrared Transmission: The Link Budget Compared to RF. IEEE Wireless Communications Magazine, 8–14 (April 2003)
2. Castillo-Vazquez, M., Puerta-Notario, A.: Single-Channel Imaging Receiver for Optical Wireless Communications. IEEE Comm. Letters 9(10), 897–899 (2005)
3. Kahn, J.M., You, R., et al.: Imaging Diversity Receivers for High-Speed Infrared Wireless Communication. IEEE Communications Magazine 36, 88–94 (1998)
4. European Standard EN 60825-1:2007 edition 2: Safety of Laser Products - Part 1: Equipement classification and requirements (2007)
5. Wolf, M., Grobe, L., Li, J.: Choice of Modulation for Gbps Wireless Infrared Systems. IPHOBAC (2009)
6. Grobe, L., Li, J., Wolf, M., Haardt, M.: Modulation and Coding Aspects for Home Gigabit Access (OMEGA) using Wireless Infrared. In: 54th Int. Scientific Colloquium (2009)
7. Li, J., Wolf, M., Haardt, M.: Investigation of the Baseline Wander Effect on Gbps Wireless Infrared System Employing 8B10B Coding. In: Int. Conference on Telecommunications (2009)

8. Agata, A., Tanaka, K., Edagawa, N.: Study on the Optimum Reed-Solomon-Based FEC Codes for 40-Gb/s-Based Ultralong-Distance WDM Transmission. Journal of Lightwave Technology 20(12), 2189–2195 (2002)
9. Muoi, T.v.: Receiver Design for High-Speed Optical-Fiber Systems. Journal of Lightwave Technology LT-2(3), 243–267 (1984)
10. CENTRONIC Limited: High Performance Silicon Photodetectors (Catalouge), 3rd edn. Centronic House, England (1996)
11. Wolf, M.: Zur breitbandigen Infrarot-Indoorkommunikation. Ph.D. thesis, Ilmenau University of Technology (2002)
12. O'Brien, D.C., Faulkner, G.E., et al.: Integrated Transceivers for Optical Wireless Communications. IEEE Journal of Selected Topics in Quantum Electronics, 173–183 (2005)
13. Agrawal, G.: Lightwave Technology: Components and Devices. John Wiley & Sons, Inc., Hoboken (2004)
14. Rechtsteiner, G., Ganske, J.: Using Natural and Artifical Light to Illustrate Quantum Mechanical Components. Chem. Educator 3(4) (1998)
15. Djahani, P., Kahn, J.M.: Analysis of Infrared Wireless Links Employing Multi-Beam Transmitters and Imaging Diversity Receivers. IEEE Transactions on Communications 48, 2077–2088 (2000)

Appendix

Table 1. Parameters used for link budget estimation based on the system presented in [6,7]

bit rate R_b in Mbps (8B/10B coded)	1250	
bit error rate p_b	10^{-9}	
photodiode	**Si**	**InGaAs**
wavelength in nm	800	1300
capacitance per area $C_\mathrm{D}/A_\mathrm{D}$ in pF/mm^2	5	60
responsivity R_λ in A/W	0.5	0.8
APD gain M	optimized between 1 and 100	
excess noise factor x_{APD}	0.3	0.7
radiance of background light $L_{\lambda,\mathrm{bg}}$ in μW/(mm^2·sr·nm)	0.04	0.04/3
optical filter bandwidth $\Delta\lambda$ in nm	10	
refraction index n_c	1.7	
feedback resistance R_L	10 kΩ·1 pF/C_D	
absolute temperature T in K	330	
collector current I_c in mA	optimized between 0.5 and 5	
base current I_b in mA	I_c/200	
series resistances $R_\mathrm{S} + R_\mathrm{bb}$ in Ω	10	
total capacitance C_tot	$C_\mathrm{tot} = C_\mathrm{D} + C_{EB} + C_{CB}$	
BJT emitter-base and collector-base capacitance in pF	$C_{EB} = 1.1$ pF, $C_{CB} = 0.25$ pF	
Personick integrals	$I_2 = 0.502$, $I_3 = 0.0843$	

An Efficient Power Control Algorithm for Supporting Cognitive Communications in Shared Spectrum Areas

Mahdi Pirmoradian, Christos Politis, and Emmanouil A. Panaousis

Wireless Multimedia & Networking (WMN) Research Group
Kingston University London
KT1 2EE London, United Kingdom
{m.pirmoradian,c.politis,e.panaousis}@kingston.ac.uk

Abstract. The concept of *Cognitive Radio (CR)* is meant to be utilised by both licensed and license-exempt users that coexist in a shared spectrum area whenever they need to avoid causing unaffordable interference to each other by following some rules. In fact, primary users should be protected by any license-exempt transmission. To this end, power control is a pivotal mechanism to be used for interference management in these scenarios. Especially, transmit power control is a vehicle to mitigate interference, in presence of CR technology, when primary receivers are attempting to reach a desired *Signal-to Interference Noise Ratio* (SINR) level. In this work we assume that a CR network relies on the same spectrum area with a primary network. Our scope is to measure the introduced interference level caused by the CR transmitter and to properly modify its power to allow a legacy user to reach a required SINR according to location of the primary user in presence of interference. A series of results are presented to prove the efficiency of our proposed scheme.

Keywords: Power Control, Primary Users, License-exempt, Shared spectrum.

1 Introduction

In modern wireless communication systems, the number of wireless users is steadily increasing resulting to a necessary demand for more available radio spectrum. Most of the radio frequency spectrum bands are completely assigned to certain technologies and it is becoming hard to find new vacant spectrum bands to deploy new technologies or enhance the existing ones. Measurements in [1] reveal that up to 85% of the spectrum available areas are partly occupied or completely unoccupied at a given time and location. Therefore a more flexible allocation strategy could solve the spectrum scarcity problem.

The concept of *Cognitive Radio* (CR), which firstly coined by Mitola in [2], is one of the most suitable solutions to support scenarios where primary users coexist with license-exempt users at the same spectrum and location area. In this case, primary users have to be protected from any potential harmful interference caused by secondary networks. If no guarantees are provided about this, it will be hard to convince a

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 496–505, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

primary user to be connected to a primary network in presence of a license-exempt radio network. However, if the latter is based on a CR technology, interference and capacity requirements about the primary user can be satisfied.

Therefore one of the most challenging issues within the context of the CR technology is to provide the prospective primary users with guarantees about the interference and the channel's capacity that is in line with Ofcom's SURs (Spectrum Usage Rights) concept [3]. In addition, due to its spectrum sharing nature, a CR network inevitably operate in interference intensive environment and effective interference management is essential towards the mitigation of interference mainly at the side of the primary user. *Power Control* is one of the most known techniques utilised to accomplish the aforementioned goal.

Our interest in this paper lies within area of the interference mitigation at the edge of the primary network to reach a desired *SINR* level in order to support adequate Quality of Service (QoS) level, by adapting the power of the CR transmitter. The cognitive network locates in the antenna effective area of the primary network and it is not possible to avoid producing interference to the primary network. To this end, the CR transmitter that is capable of measuring the current interference at the primary network, it adjusts its transmission power to avoid harmful interference to the primary user and to acquire the appropriate channel capacity users.

This paper is structured as follows. In section 2, we discuss related work done in the area of power control. In section 3, we present the model that has been assumed in this paper. In section 4, we proposed our power control algorithm and examine the different parameters such as SINR, interference, path loss and channel capacity seen by primary user in case of a fixed size licensed spectrum network. In section 5, mathematical and simulation results are presented. Finally, in section 6 we conclude this paper and we mention ideas for future work.

2 Related Work

In [4], author presents an optimal power control method to maximize the secondary user ergodic capacity subject to a new proposed constraint to protect the primary transmission, which limits the maximum ergodic capacity loss of the primary user resulted from the CR transmissions. The fundamental capacity limits for spectrum sharing based CR networks over fading channels are studied by the author. Results reveal that the proposed policy can lead to substantial capacity gains for both the PU and SU over the conventional policy.

The light of [5], authors present a mathematical model for calculating the total unexpected by any primary receiver interference in the presence of CRs. In that work, cumulative distribution function (CDF) of the interference due to the cognitive devices is calculated meanwhile primary protected area and number of the deployed cognitive radios is computed. The results reveal if CRs have a priori knowledge of the radio environment map, the number of CRs deployed in that environment can be increase.

In [6], authors present a novel hybrid power control scheme in an Hierarchical Spectrum Sharing Network (HSSN) to fully make use of the potential of an HSSN. The proposed scheme is composed of a centralized power control scheme, a distributed power control scheme and a coordination policy to coordinate these two types of power control schemes when both of them are exploited in the same channels. Outcomes of the paper reveal that the proposed power control scheme can meet the requirements of low emission power as well as high QoS level.

3 System Model

The configuration of our system is shown in Figure 1. We consider a primary system that is surrounded by a CR network. The primary receiver is placed at the edge of the primary network and its transmitter in the centre of a circular region of radius R. As shown in Figure 1, within the protected area there is not interference and the primary users satisfy a SINR value to transmit data to the base station *(SINR>SINRt)*.

$$\sum_{\substack{j=1\\ i\neq j}}^{M} P_{ij}h_{ij} \leq I_t \tag{1}$$

The path gain h_{ij} is given by [6]

$$h_{ij} = {d_{ij}}^{-\alpha} 10^{\tau/10} \tag{2}$$

The threshold interference (I_t) in general may depend on the characteristics of the interfering signal (e.g. signal waveform, continues vs. intermittent interference).

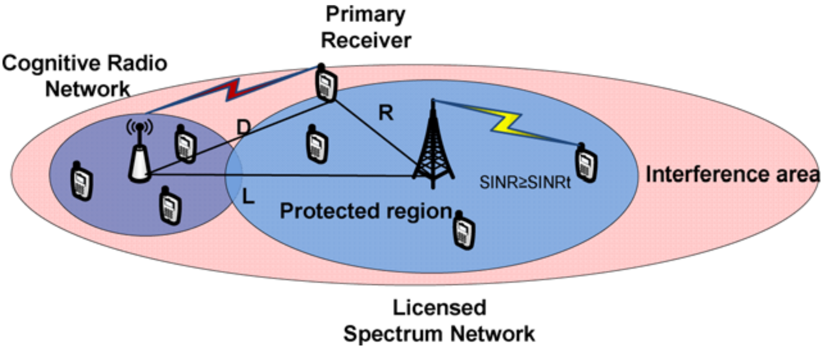


Fig. 1. Our scenario where the primary and the secondary network use the same spectrum band

The interference range depends on the CR transmitter's power and the primary receiver interference tolerance. The interference range and minimum distance between the CR transmitter and the primary receiver can be calculated as follows:

$$Dmin = (P_c 10^{\frac{\tau}{10}}/I_t)^{1/\alpha}$$

Table 1. Definition of parameters

P_{ij}	Transmitted power of transmitter *i* to receiver *j*
h_{ij}	Path gain between transmitter *i* and receiver *j*
α	Path loss factor
τ	Random variable of normal distribution
σ^2	Background noise
h_{kj}	Path gain between transmitter *k* and receiver *j*
I_t	Minimum interference that primary user can tolerate in channel *j*
d	Distance between transmitter *i* and receiver *j*
M	Number of transmitter
$SINRt$	Necessary SINR to support QoS

The first goal of this work is to mitigate the harmful interference caused by the CR transmitter to the primary users. It is required that the total transmitted power of the CR should not exceed an interference constraint.

The received power by the primary user should be written as:

$$Pr = Pt.d^{-\alpha}10^{\tau/10}$$

Where Pt denotes the power of the transmitter (license-exempt user). Consequently, the interference to the primary user should be:

$$I_p = \sum_{\substack{j=1 \\ j\neq i}}^{M} d_{ij}^{-\alpha} P_j 10^{\tau/10}$$

The second scope of this work is to optimize the primary user's QoS level based on its position. Considering the SINR requirements as the basic QoS metric, the received SINR must exceed a desired threshold in order the legacy user to recover correctly the received data. We define *SINRt* the minimum value at which the primary receiver has the minimum required QoS level to support is communication link. Thus, the SINR of the primary user *i* could be expressed by:

$$SINR_i = \frac{P_{ij}h_{ij}}{\sigma^2 + \sum_{\substack{k=1 \\ k\neq i}}^{M} P_{kj}h_{kj}} \geq SINRt \tag{3}$$

Moreover, the value of the channel capacity indicates the level of the QoS at the side of the primary user and can be expressed by:

$$C = B\log_2(1 + SINR)\ \text{bps}$$

To achieve the required SINR and the QoS level of the primary receiver's communication link, a nonlinear program can be satisfied the requirements as follows:

$$\text{Maximise }\ SINRi = \frac{P_{ij}h_{ij}}{\sigma^2 + \sum_{\substack{k=1 \\ k\neq i}}^{M} P_{kj}h_{kj}} \geq SINRt$$

$$\text{Subject to}\begin{cases}\sum_{\substack{j=1\\ i\neq j}}^{M} P_{ij}h_{ij} \le I_t\\ 0 < P_c \le P_{cmax}\end{cases} \tag{4}$$

4 Proposed Methodology

In this section, we mathematically calculate the SINR and the channel capacity at the licensed user. Our solution is based on the position of the primary user and the CR transmitter. In this scenario the CR network attempts to utilize the spectrum thus causing harmful interference to the primary user. We assume the primary network's base station as highlighted in Figure 2. The position of the primary user each time can be expressed by:

$$\Delta = r\measuredangle\theta, \text{ Then } \Delta_x = r\cos\theta, \Delta_y = r\sin\theta$$

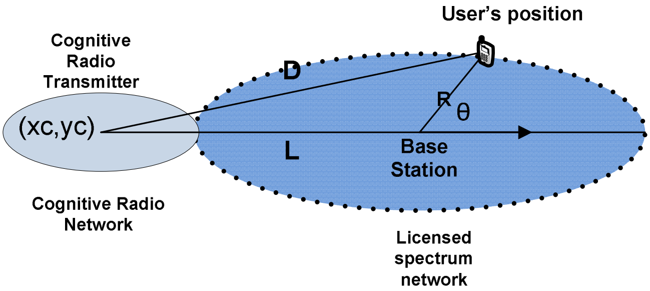


Fig. 2. Mathematic and geometric explanation of the system model

$$D = \sqrt{\left((x_c-\Delta_x)^2 + \left(y_c-\Delta_y\right)^2\right)}$$

Getting D into equation (2)

$$h_{cp} = (\sqrt{\left((x_c-\Delta_x)^2 + \left(y_c-\Delta_y\right)^2\right)})^{-\alpha}10^{\tau/10}$$

Where h_{cp} denotes the *path gain* between the primary receiver and the CR transmitter. By recalling the SINR formula at the primary receiver:

$$SINR_p = \frac{P_{BS}R^{-\alpha}10^{\tau/10}}{\sigma^2 + P_c D^{-\alpha}10^{\tau/10}} \tag{5}$$

The minimum SINR occurs when $D = Dmin$ namely θ is equal to:

$$\frac{\partial D}{\partial \theta} = 0 \implies \theta = -\tan^{-1}(\frac{y_c}{x_c})$$

The adjusted power of the CR due to *SINRt* of the primary user is given by:

$$P_c = (\frac{\left(P_{BS}R^{-\alpha}10^{\frac{\tau}{10}}\right)}{SINRt} - \sigma^2)D^{\alpha}10^{-\tau/10} \quad (6)$$

According to the mathematic results, Table 2 highlights our algorithm to support enough QoS level at the side of the licensed user while providing services to a license-exempt user.

Table 2. Power Control algorithm of the CR transmitter

```
Algorithm:
    1. Initialize power of the CR to maximum
    2. Calculate primary receiver's SINR Interference and
    channel capacity
    3. If SINR<SINRt
    Decrease $P_c$ to approach desire SINR
    Go to 2
    Else
    $P_c$ set to $P_{cmax}$ and calculate channel capacity
    4. Change position of primary receiver
    5. End loop
    Return $P_c$, SINR, C
```

Table 3. The simulation parameters

P_c	Power of the CR transmitter	17dBm
P_{BS}	Power of the primary transmitter	30dBm
SINRt	Minimum required SINR	10dB
τ	Random variable of normal distribution	0 dB
α	Path loss exponent	2
L	Distance between primary and CR transmitters	1500m
B	Band width	1 Mhz
σ^2	Noise power	10^{-8}
R	Maximum primary network's radius	1000m
R0	Maximum CR network's radius	100m

5 Performance Evaluation

The formulas presented in the previous sections provide analytical outcome of the expected system. Some prominent parameter's values are mentioned in table 3. Considered that the system uses M-ary Quadrature Amplitude Modulation (MQAM) with 64-QAM. Analytical results in Figure 3 reveal that the *SINR* and the channel's capacity of primary receiver vary according to the different positions of the licensed user. Moreover, a minimum SINR value equal to 7dB occurs when the licensed user is at the closest to CR transmitter point ($\theta = \pi$). At the same time, ($\theta = \pi$), power of the cognitive transmitter at maximum level is 17dBm. Simultaneously, channel capacity is reduced to a minimum value. Results indicate that the harmful interference introduced to the receiver by the CR transmitter and that the *SINR* reaches a low level value (less than *SINRt*). According to *SINR* requirement on the path and the fixed distance between CR transmitter and primary base station, the power of the CR can be adjusted to achieve the desired level of *SINR*.

It is clear that, due to required *SINR* at the primary user, the power of the CR should be controlled to approach desired value. We above noted that the power algorithm increases the performance of the primary receiver by mitigating the harmful interference. Indeed, in the following figures we have illustrated the performance evaluation of our simulations. For this purpose, we used our custom simulator developed using the MATLAB programming language.

In Figure 3 variations of the primary receiver's *SINR* depicts that the minimum value of the *SINR* equals to 7dB and occurs at ($\theta = \pi$), at this situation power of the CR is 17dBm. Approximately variation of the *SINR* from farthest position to the closest place of the CR transmitter is 9dB.

The curve in Figure 4 reveals the capacity channel of the primary receiver varies from maximum 6 Mbps to minimum 2.5 Mbps at closest point to the CR transmitter with 17dBm power. The receiver's capacity channel altering is 3.5 Mbps, it shows the harmful interference affects primary receiver at $\theta = \pi$.

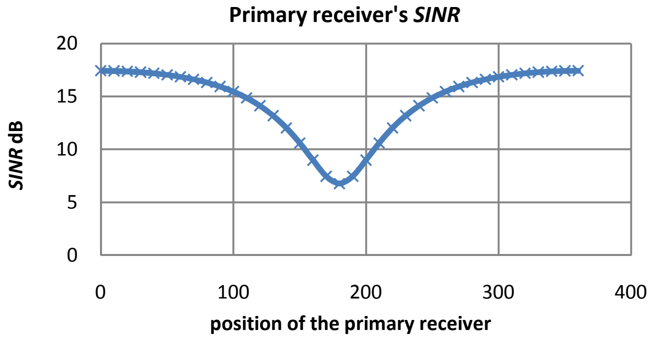


Fig. 3. Presence of CR transmitter and variation of the primary receiver's SINR (distance from primary transmitter is 1000m)

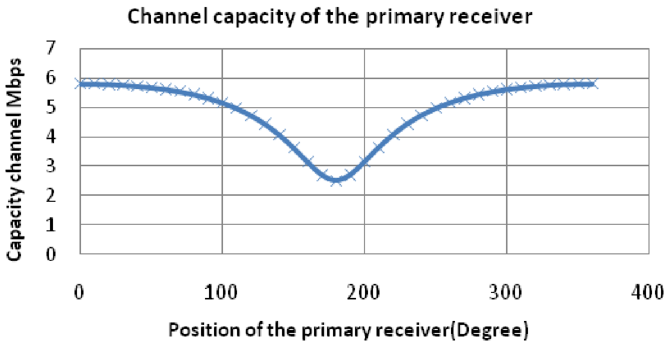


Fig. 4. CR transmitter existence and channel capacity variation at primary receiver

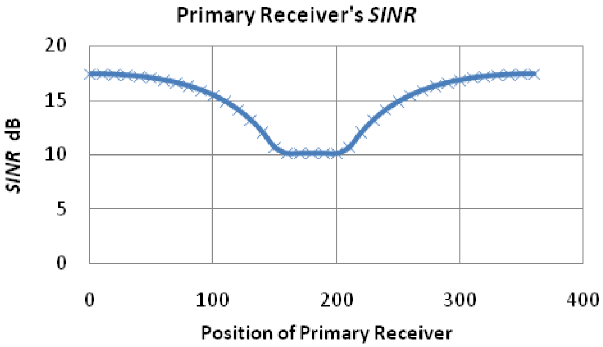


Fig. 5. Primary receiver's *SINR* adapt on minimum *SINR* according to get suit QoS level

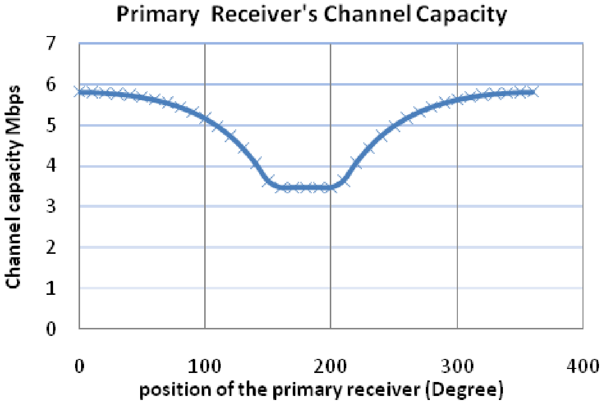


Fig. 6. Improving the QoS level of the primary receiver with respect to CR transmitter's power

In Figure 5 we depict the *SINR* of the primary receiver is reaching to the *SINRt* (10dB) due to adjusting power of the CR transmitter. As numerical results show the minimum power of the CR is 13dBm to approach minimum interference at ($\theta = \pi$) (see Figure 7) meanwhile channel capacity of the receiver is 3.8 Mbps. It reveals the capacity optimizes amount 1.3 Mbps at that position (see Figure 6). As shown, in last three Figures (5, 6 and 7), while the primary receiver gets into the harmful interference area$5\pi/6 \leq \theta \leq 7\pi/6$, the power of the secondary transmitter should be adjusted.

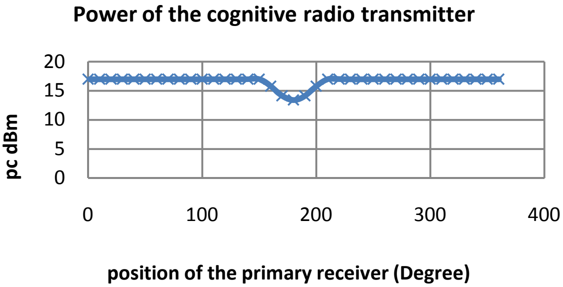


Fig. 7. CR transmitter's power and mitigate harmful interference to primary receiver

6 Conclusions

In this work, we show that according to the location of a CR transmitter and its power, the performance of a primary user in terms of *SINR* and interference can be maximized. Although several methods have been used to mitigate interference we chose to implement a power control mechanism in this paper. The results show that to achieve minimum *SINR* namely 10dB at the primary user, the power of the CR transmitter should reach the value of 13dBm when the licensed user is at the closest to the CR transmitter position. Concurrently, the channel capacity reaches the value of 3.8 Mbps.

In future work, we plan to simulate several CRs that will share the common spectrum with a primary user and they will be laid in the critical common interference area. Then interference aggregated to a primary receiver will be mitigated towards the enhancement of the licensed CR user's QoS level.

References

1. Spectrum Policy Task Force Report (ET Docket-135), Federal Communications Comsssion, Tech. Rep. (2002), `http://hraunfoss.fcc.gov/edocspublic/attachmatch/DOC-228542A1.pdf`
2. Mitola, J., Maguire, G.Q.: Cognitive radio: making software radios more personal. IEEE Personal Communications 6(4), 13–18 (1999)

3. A Study into the Application of Interference Cancellation Techniques. A study of Ofcom, vol. 2 (April 2006)
4. Zhang, R.: Optimal Power Control over Fading Cognitive Radio Channels by Exploiting Primary User CSI. In: Proc. IEEE Global Communication Conference (IEEE GLOBECOM 2008), New Orleans, USA (2008)
5. Hanif, M.F., Shafi, M., Smith, P.J., Dmochowski, P.A.: Interference and Deployment Issues for Cognitive Radio Systems in Shadowing Environments. CoRR abs/0905.3023 (2009)
6. Hayar, A., Porrat, D., Zheng, H., Zhang, H., Nandagopalan, S.S.(eds.): Physical Communication. Cognitive Radio Networks: Algorithms and System Design 2(1-2), 1–2 (2009), doi:10.1016/j.phycom.2009.04.001

TOA Estimation in UWB: Comparison between Time and Frequency Domain Processing

Eva Lagunas[1], Lorenzo Taponecco[3], Montse Nájar[1,2], and Antonio D'Amico[3]

[1] Department of Signal Theory and Communications, Universitat Politècnica de Catalunya (UPC), C/ Jordi Girona 1-3, 08034, Barcelona, Spain
{eva.lagunas,montse.najar}@upc.edu
[2] Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Av. Canal Olmpic, Castelldefels, Spain
[3] Department of Information Engineering, Università di Pisa, Via G. Caruso 16, 56122, Pisa , Italy
{lorenzo.taponecco,antonio.damico}@iet.unipi.it

Abstract. A comparison between time and frequency domain TOA estimators compliant with the 802.15.4a Standard has been made. The time domain estimator is done in two stages. One has the goal of identify the first pulse in each symbol interval and the other aims to acquire the start of frame delimiter. The frequency domain estimator is also based in two stages. A simple coarse estimation stage provides the symbol synchronization required by the fine estimation stage which finds the first delay of the first arriving path in a power delay profile developed in the frequency domain by using high resolution spectral estimation techniques. An accuracy of few centimeters is asymptotically achieved by both estimators. While time domain estimator shows slightly more accurate results at high values of SNR, frequency domain estimators works slightly better at low SNR.[1]

Keywords: Time of Arrival estimation, Ultra-Wide Band, IEEE 802.15.4a Standard, frequency domain, time domain.

1 Introduction

Localization and Positioning represents one of the main themes that are being developed in the field of wireless communications. One of the existing technologies that offers better features related to the location applications is Ultra-Wideband (UWB). UWB signals can be used for accurate time of arrival (TOA) based ranging because of their high time resolution. The TOA approach estimates the time of flight of the first arriving path and thus acquires the distance information

---

[1] This work was partially supported by the Departament d'Universitats, Recerca i Societat de la Informació de la Generalitat de Catalunya, by the Catalan Government under grant 2009 SGR 891, by the Spanish Government under project TEC2008-06327-C03 (MULTI-ADAPTIVE) and by the European Commission under project NEWCOM++ (ICT-FP7-216715).

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 506–517, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

between a pair of nodes by multiplying the travel time by the speed of the light. The TOA estimation accuracy depends on how precisely the receiver can discriminate the first arriving signal, which in a multipath environment may not be the strongest.

This work discusses two ranging algorithms for impulse radio UWB signals compliant with the IEEE 802.15.4a standard. The first one is described in [1]- [2]. It proposes a ranging algorithm for non-coherent receivers based on the preamble of the IEEE 802.15.4a standard. The ranging problem consists in estimating the TOA of the first pulse of the PHR (the ranging marker). The estimation is done in a two-step procedure which first leads to a coarse estimate and then to a finer results. The second estimator considers a frequency domain approach based on the algorithm proposed in [3]- [4] which has been adapted to comply with the IEEE 802.15.4a. The estimator is performed in two stages. First a coarse estimation is done in order to provide the time reference for symbol synchronization and then, working in the frequency domain, a high resolution estimation of the first arriving path is done in the second stage.

2 System Model

The standard specifies two optional signalling formats based on Impulse-Radio UWB (IR-UWB) and Chip Spread Spectrum (CSS). The IR-UWB option targets mainly for ranging whereas the CSS signals have better features for data communication. Since we investigate ranging for the IEEE 802.15.4a standard we only focus on the IR-UWB option. The frame format structure is shown in Fig. 1.

The standard packet consists of a synchronization header (SHR) preamble, a physical layer header (PHR) and a data field (PSDU). The SHR preamble is composed of the ranging (SYNCH) preamble and the start of frame delimiter (SFD).

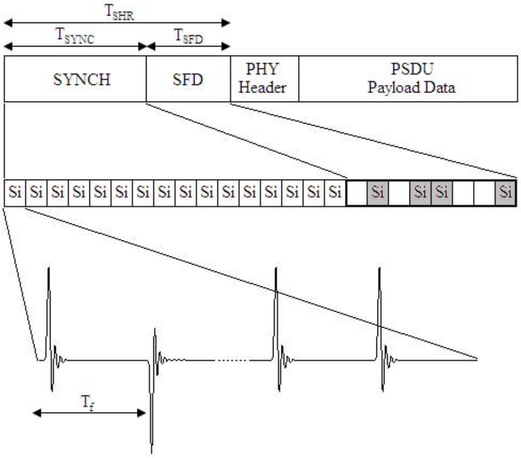


Fig. 1. Frame format structure

The ranging preamble can consist of 16,64,1024,4096 symbols. The underlying symbol of the ranging preamble uses one of the length-31 ternary sequences, c_i. Each c_i of length $K_{pbs} = 31$ contains 15 zeros and 16 non-zero codes, and has the desired property of perfect periodic autocorrelation. The PHR consists of 19 bits and conveys information necessary for a successful decoding of the packet to the receiver.

The mathematical model of the signal transmitted during the SHR is,

$$s(t) = \sum_{k=0}^{N_{SYNC}+N_{SFD}-1} a_k \psi(t - kT_{sym}) \tag{1}$$

where N_{SYNC} and N_{SFD} are the lengths of the SYNC and the SFD and T_{sym} is the symbol duration. Coefficients a_k are all equal to 1 during the SYNC while they take values $\{-1, 0, +1\}$ during the SFD. Finally $\psi(t)$ is expressed as,

$$\psi(t) = \sum_{j=0}^{K_{pbs}-1} c_j p(t - jT_f) \tag{2}$$

In this equation $p(t)$ is an ultrashort pulse (monocycle) and $T_f = T_{sym}/K_{pbs}$ is the pulse repetition period.

Signal $s(t)$ propagates through an L-path fading channel whose response to $p(t)$ is $\sum_{l=0}^{L-1} h_l p(t - \tau_l)$. Note that it is assumed that the received pulse from each l-th path exhibits the same waveform but experiences a different fading coefficient, h_l, and a different delay, τ_l. Without loss of generality we assume $\tau_0 \leq \tau_1 \leq \ldots \leq \tau_{L-1}$. The received waveform can be written as,

$$r(t) = \sum_{k=0}^{N_{SHR}-1} \sum_{j=0}^{K_{pbs}-1} \sum_{l=0}^{L-1} a_k c_j h_l p(t - T_k^j - \tau_l) + w(t) \tag{3}$$

where $w(t)$ is thermal noise with two-sided power spectral density $No/2$, $T_k^j = jT_f + kT_{sym}$ and $N_{SHR} = N_{SYNC} + N_{SFD}$.

3 Frequency Domain TOA Estimation

Next, the frequency domain TOA estimator [3] is described in detail for completeness. The block diagram of the frequency domain TOA estimator is sketched in Fig. 2. For the purpose of describing the estimation algorithm the receiver assumes an ideal Band Pass Filter (BPF) sampled at Nyquist rate, followed by a Discrete Fourier Transform (DFT) module that transforms the signal to the frequency domain. The frequency samples are processed in the TOA estimator stage without knowledge of the specific pulse shape at the output of the BPF. The fine TOA estimator requires a previous stage that provides a coarse symbol synchronization. Note that this receiver scheme is a non-coherent receiver.

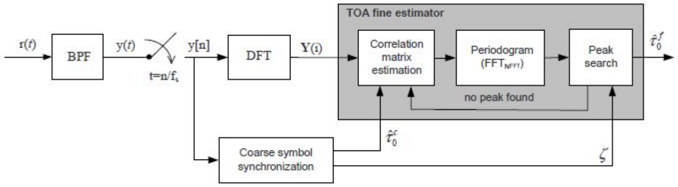


Fig. 2. Block diagram of the non-coherent receiver

The signal associated to the j-th transmitted pulse corresponding to the k-th symbol, in the frequency domain yields:

$$Y_j^k(w) = \sum_{l=0}^{L-1} a_k c_j h_l S_j^k(w) e^{-jw\tau_l} + V_j^k(w) \tag{4}$$

with,

$$S_j^k(w) = \tilde{P}(w) e^{-jw((kN_f+j)T_f} \tag{5}$$

where $\tilde{P}$ denotes the Fourier Transform of $\tilde{p}(t)$ which is the received pulse waveform at the output of the BPF and N_f is the number of frames per symbol. $V_j^k(w)$ is the noise in the frequency domain associated to the j-th frame interval correspondig to the k-th symbol. Sampling (4) at $w_n = w_0 n$ for $n = 0, 1, \ldots, N-1$ and $w_0 = 2\pi/N$ and rearranging the frequency domain samples $Y_j^k[n]$ into the vector $\mathbf{Y}_j^k \in \mathbb{C}^{N\times 1}$ yields,

$$\mathbf{Y}_j^k = a_k c_j \mathbf{S}_j^k \mathbf{E}_\tau \mathbf{h} + \mathbf{V}_j^k \tag{6}$$

where the matrix $\mathbf{S}_j^k \in \mathbb{C}^{N\times N}$ is a diagonal matrix whose components are the frequency samples of $S_j^k(w)$ and the matrix $\mathbf{E}_\tau \in \mathbb{C}^{N\times L}$ contains the delay-signature vectors associated to each arriving delayed signal,

$$\mathbf{E}_\tau = \left[\mathbf{e}_{\tau_0} \ldots \mathbf{e}_{\tau_j} \ldots \mathbf{e}_{\tau_{L-1}}\right] \tag{7}$$

with $\mathbf{e}_{\tau_j} = \left[1\; e^{-jw_0\tau_j} \ldots e^{-jw_0(N-1)\tau_j}\right]^T$. The channel fading coefficients are arranged in the vector $\mathbf{h} = \left[h_0 \ldots h_{L-1}\right]^T \in \mathbb{C}^{L\times 1}$, and the noise samples in vector $\mathbf{V}_j^k \in \mathbb{C}^{N\times 1}$.

Estimation of the TOA from the noisy observation $y(t)$ without knowledge of the specific pulse shape $\tilde{p}(t)$ is the goal of the algorithm [4]- [3]. First, a simple coarse estimation stage that provides the time reference for a symbol synchronization and estimates the threshold used in the TOA algorithm is developed. The frequency domain samples are then processed in the fine TOA estimator stage. The resolution of the algorithm is given by the pulse time width.

3.1 Coarse TOA Estimation

The coarse estimation consists of an energy estimator and a simple search algorithm that identifies the beginning of the symbol by applying a minimum distance criterion. Since the signal structure in the Standard does not include a time hopping sequence, the minimum distance criterion is applied in this case based on the ternary sequence knowledge, c_i, at symbol level.

It is assumed that the acquisition begins at any point of the SYNCH preamble t_0 and lasts K_s+1 symbols. Note that the acquisition window duration is defined one symbol longer than the number of symbols considered for the fine timing estimation.

To find the beginning of the next symbol the frame number which the first detected pulse belongs to is needed. Lets denote $y[m] = y(mT_s)$ the discrete-time received signal, where T_s is the sampling period. The time domain samples of the received signal in the i-th frame time interval are defined as,

$$y_{frame,i}[n] = y[(i-1)K_f + n] \quad \text{for} \quad n = 1, \ldots, K_f \tag{8}$$

where $i = 1, \ldots, N_f(K_s+1)$. Rearranging the time domain samples $y_{frame,i}[n]$ in the vector $\mathbf{y}_{frame,i} \in \mathbb{C}^{K_f \times 1}$, being $K_f = \lfloor T_f/T_s \rfloor$ the number of samples in a frame interval, the energy at each frame interval in one symbol period is obtained averaging for each of the N_f frames, over all K_s+1 symbols in the acquisition interval. That is,

$$E_{frame,j} = \sum_{k=0}^{K_s} \left\| \mathbf{y}_{frame,j+31k} \right\|^2 \qquad j = 1, \ldots, N_f \tag{9}$$

Although the energy estimation is done in the temporal domain, it can be also obtained in the frequency domain. Then the algorithm searches the 16 maxima corresponding to the 16 frames containing pulses and estimates the ternary sequence $\hat{c}_i$. From the original ternary sequence c_i it is defined the vector $\mathbf{d}$ as a vector composed of the 16 positions of the sequence c_i containing ±1. Then it is defined circulant matrix $\Delta_{\rho_{c_i}}$ whose rows contain the relative delays in number of frame intervals between two consecutive pulses within a symbol period. Each row is a shifted version of the previous one. More specifically, defining $\rho_{c_i}(n) = d(n+1) - d(n) - 1$ for $n = 1, \ldots, 15$ and $\rho_{c_i}(16) = 31 - d(16) + d(1)$ as the number of frames between two consecutive transmitted pulses, the circulant matrix $\Delta_{\rho_{c_i}}$ is given by,

$$\Delta_{\rho_{c_i}} = \begin{bmatrix} \rho_{c_i}(1) & \rho_{c_i}(2) & \ldots & \rho_{c_i}(15) & \rho_{c_i}(16) \\ \rho_{c_i}(2) & \rho_{c_i}(3) & \ldots & \rho_{c_i}(16) & \rho_{c_i}(1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \rho_{c_i}(16) & \rho_{c_i}(1) & \ldots & \rho_{c_i}(14) & \rho_{c_i}(15) \end{bmatrix} \tag{10}$$

Hence, with the estimated ternary sequence $\hat{c}_i$ it is conformed the vector $\hat{d}$ which contains the estimated pulses positions or, in other words, which contains the

16 positions of the estimated sequence $\hat{c}_i$ containing ±1. Therefore, the relative distance between the 16 estimated positions of the pulses form the vector,

$$\varDelta d = \left[\hat{\rho}_{c_i}(1)\ \hat{\rho}_{c_i}(2)\ \ldots\ \hat{\rho}_{c_i}(15)\ \hat{\rho}_{c_i}(16)\right] \tag{11}$$

If we denote the first pulse within the symbol with the number 1, the second with the number 2 and so on until the sixteenth pulse with the number 16, then the estimated number of the first detected pulse $\eta \in \left\{1, \ldots, 16\right\}$ is carried out by finding the closest row of $\varDelta_{\rho_{c_i}}$ which provides lower mean square error with respect to $\varDelta d$,

$$\eta = \arg \min_{j=1,\ldots,16} \left\| \varDelta d - \varDelta_{\rho_{c_i}}|_j \right\|^2 \tag{12}$$

where $\varDelta_{\rho_{c_i}}|_j$ denotes the j-th row of the matrix $\varDelta_{\rho_{c_i}}$. From the estimated pulse number η it is estimated the frame number $\upsilon \in \left\{1, \ldots, 31\right\}$ which the first detected pulse belongs to. That is,

$$\upsilon = d(\eta) - \hat{d}(1) + 1 \tag{13}$$

Then the TOA coarse estimation can be directly identified as,

$$\widehat{\tau}_0^c = (31 - \upsilon + 1)T_f \tag{14}$$

The temporal resolution of this estimation is a frame period T_f.

3.2 Fine TOA Estimation

Once the beginning of the symbol is coarsely estimated, working in the frequency domain high resolution spectral estimation techniques can be applied to obtain a signal power profile, defined as the signal energy distribution with respect to the propagation delays, from which the TOA is estimated.

The fine estimation $\hat{\tau}_0$ is obtained from the TOA coarse estimation $\hat{\tau}_0^c$ and a high resolution time delay $\tilde{\tau}$ estimate of the first arriving path with respect to the time reference obtained in the coarse estimation stage.

$$\hat{\tau}_0 = \hat{\tau}_0^c + \tilde{\tau} \tag{15}$$

The fine estimator consist of finding the first delay, $\tilde{\tau}$, that exceeds a given threshold, P_{th}, in the power profile,

$$\tilde{\tau} = \min \arg_\tau \left\{P(\tau) > P_{th}\right\} \tag{16}$$

Given the signal frequency domain structure obtained in (6), the power delay profile can be obtained by estimating the energy of the frequency domain signal filtered by the delay signature vector, $\mathbf{e}_\tau$, at each time delay resulting in the quadratic form,

$$P(\tau) = \mathbf{e}_\tau^H \mathbf{R} \mathbf{e}_\tau \tag{17}$$

where $\mathbf{R}$ is the frequency domain signal correlation matrix.

The quadratic form ([17]) allows for a low complexity implementation by applying the Fast Fourier Transform (FFT) to the following coefficients,

$$\tilde{R}_n = \begin{Bmatrix} \sum_{k=n+1}^{N} \mathbf{R}_{k-n,k} & : & 0 \leq n \leq N-1 \\ \sum_{k=1}^{N+n} \mathbf{R}_{k-n,k} & : & -N+1 \leq n \leq 0 \end{Bmatrix} \tag{18}$$

where $\tilde{R}_n$ is the sum of the n-th diagonal elements of the correlation matrix $\mathbf{R}$. So, the maximization problem resorts to maximize the following expression,

$$P(\tau) = \sum_{n=1-N}^{-N+1} \tilde{R}_n e^{-jw_0 \tau n} \tag{19}$$

The number of points used in the DFT is equivalent to the number of values of τ to sweep. Therefore, the more points used more accurate will the TOA estimation be.

In order to obtain a more robust estimation of the correlation matrix $\mathbf{R}$, it can be obtained averaging over K_s symbols. The expression is,

$$\mathbf{R} = \frac{1}{N_f K_s} \sum_{k=1}^{K_s} \sum_{j=1}^{N_f} \mathbf{Y}_{jq}^{k} {\mathbf{Y}_{jq}^{k}}^{H} \tag{20}$$

Note that the computation of the correlation matrix also takes advantage of the inherent temporal diversity of the IR-UWB signal, with N_f repeated transmitted pulses for each information symbol, by computing the correlation matrix over the N_f received frames.

4 Time Domain TOA Estimation

The time domain TOA Estimator is based on the receiver's block diagram sketched in Fig. [3].

The incoming waveform $r(t)$ is first passed through a BPF with center frequency f_0 and then is demodulated in a square-law device followed by a low-pass filter (LPF). The proposed ranging algorithm is based on the observation of the LPF output, which is conveniently expressed by introducing the notion of the complex envelope of a bandpass signal.

Call $g_l(t)$ the convolution of $p_l(t)$ with the BPF impulse response, where $p_l(t) = h_l p(t)$. Now define

$$u(t) = \sum_{l=0}^{L-1} g_l(t - (\tau_l - \tau_0)) \tag{21}$$

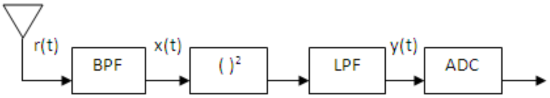


Fig. 3. Block diagram of the non-coherent receiver

Next assume that: (a) LPF has a rectangular transfer function with a bandwidth sufficiently large to pass $|\breve{x}(t)|^2$ undistorted; (b) the duration of $\breve{u(t)}$ is shorter than T_f. Putting these facts together, after some manipulations it is found that the LPF output $u(t)$ can be written as the sum of a signal component $s_y(t)$ plus a noise component $n_y(t)$, with

$$s_y(t) = \sum_{k=0}^{N_{SHR}-1} \sum_{j=0}^{K_{pbs}-1} c_j^2 q(t - T_k^j - \tau_0) \tag{22}$$

and $q(t) = |\breve{u}(t)|^2$. Note that $q(t)$ is non-negative pulse with support $[0, T_f)$ as a consequence of (b). Its shape is unknown and depends on the channel response.

As was done with the frequency domain estimator we assume that presence of a frame has been signaled at some time t_0 and that the estimator disposes of K_s symbols. The TOA estimation is divided in two steps. In the first one (*highest-peak search*) we estimate the delay τ_h (relative to t_0) of the highest peak in the first $q(t)$-pulse of the generic symbol N. As is shown in Fig. 3, τ_h exceeds τ by some quantity Δ, i.e., $\tau_h = \tau + \Delta$. In the second step (*leading-path search*) we start from the highest peak already found and, as in [5], we jump back by T_{back} seconds to an instant prior to the beginning of the $q(t)$-pulse. Then, we perform a forward search looking for the first appearance of the $q(t)$-pulse energy. This provides Δ, and τ is computed as $\tau = \tau_h - \Delta$.

4.1 Highest-Peak Search

To begin the Highest-Peak Search we write τ_h as $\tau_h = mT_f + \varepsilon$, with $0 \leq m \leq K_{pbs} - 1$ and $0 \leq \varepsilon < T_f$, and we look for the values of m and ε. To this end, indicating with $\tilde{m}$ and $\tilde{\varepsilon}$ trial values of these parameters, we concentrate on the following function

$$S(\tilde{m}, \tilde{\varepsilon}) \triangleq \frac{1}{K_s} \sum_{i=0}^{K_s-1} \sum_{k=0}^{K_{pbs}-1} d^2_{|k-\tilde{m}|_{K_{pbs}}} s_y(t_0 + \tilde{\varepsilon} + T_k^j) \tag{23}$$

where $|a|_b \triangleq a$ modulo b. As is now explained, its expectation $E\{S(\tilde{m}, \tilde{\varepsilon})\}$ over the thermal noise allows one to compute m and ε. In fact, long calculations (omitted for space limitations) yield

$$E\{S(\tilde{m}, \tilde{\varepsilon})\} = q(|\Delta + \tilde{\varepsilon} - \varepsilon|_{T_f}) \sum_{k=0}^{K_{pbs}-1} d^2_{|k-\tilde{m}|_{K_{pbs}}} d^2_{|k-\mu(\tilde{\varepsilon})|_{K_{pbs}}} + 2\sigma^2 K_{\pm 1} \tag{24}$$

where σ^2 is the noise power at the BPF output, $K_{\pm 1}$ is the number of non-zero elements of sequence $\{d_k\}_{k=0}^{K_{pbs}-1}$, and $\mu(\tilde{\varepsilon})$ is an integer defined as

$$\mu(\tilde{\varepsilon}) \triangleq m - \left\lfloor \frac{\Delta + \tilde{\varepsilon} - \varepsilon}{T_f} \right\rfloor \tag{25}$$

where $\lfloor x \rfloor$ is the integral part of x. We maintain that $E\{S(\tilde{m}, \tilde{\varepsilon})\}$ achieves its absolute maximum for $\tilde{m} = m$ and $\tilde{\varepsilon} = \varepsilon$. This is seen by inspection of (24), bearing in mind that: (i) since $\Delta < T_f$ we have $\lfloor \Delta / T_f \rfloor = 0$ and $|\Delta|_{T_f} = \Delta$; (ii) as $q(t)$ has its highest peak at $t = \Delta$ (see Fig. 3), $q(|\Delta + \tilde{\varepsilon} - \varepsilon|_{T_f})$ has its maximum at $\tilde{\varepsilon} = \varepsilon$; (iii) for $\tilde{\varepsilon} = \varepsilon$ equation (25) gives $\mu(\tilde{\varepsilon}) = m$ and the summation in (24) achieves its highest value for $\tilde{m} = m$.

In conclusion, if $E\{S(\tilde{m}, \tilde{\varepsilon})\}$ were available, m and ε (and hence $\tau_h = mT_f + \varepsilon$) could be exactly computed. As this is not the case, however, we must content ourselves with estimates. To this end we first replace $S(\tilde{m}, \tilde{\varepsilon})$ with a modified version obtained by sampling $s_y(t)$ at a suitable rate $1/T_s$ and, next, we maximize this version instead of $E\{S(\tilde{m}, \tilde{\varepsilon})\}$. In summary, we call $t_\ell = t_0 + \ell T_s$ $(\ell = 0, 1, 2, ...)$ the sampling instants and we assume T_s a sub-multiple of T_f, say $T_f / T_s = N_s$. Then, letting $\tilde{\varepsilon} = \tilde{n} T_s$ into the right hand side of (23) yields a quantity expressed in terms of the $s_y(t)$-samples. The estimates $\hat{m}$ and $\hat{\varepsilon}$ are obtained by maximizing this quantity for $0 \leq \tilde{m} < K_{pbs} - 1$ and $0 \leq \tilde{n} < N_s - 1$.

4.2 Leading-Path Search

Having estimated the delay τ_h (relative to t_0) of the highest peak of the first $q(t)$-pulse in the symbol N, we can deal with the Leading-Path Search where we look for the delay τ of the starting time of the same pulse (see Fig. 3). This can be done by measuring the difference $\Delta = \tau_h - \tau$. To simplify the discussion we assume that the estimate $\hat{\tau}_h$ of τ_h is perfect (i.e., $\hat{m} = m$ and $\hat{\varepsilon} = \varepsilon$), with the understanding that the replacements $m \to \hat{m}$ and $\varepsilon \to \hat{\varepsilon}$ must be made in the final result.

To begin, consider (23) as computed for $\tilde{m} = m$

$$S(m, \tilde{\varepsilon}) = \frac{1}{K_s} \sum_{i=0}^{K_s - 1} \sum_{k=0}^{K_{pbs} - 1} d^2_{|k-m|_{K_{pbs}}} s_y(t_0 + \tilde{\varepsilon} + T_k^j) \tag{26}$$

Fig. 4 shows a realization of $S(m, \tilde{\varepsilon})$ in the absence of noise. The interval $0 \leq \tilde{\varepsilon} \leq T_f$ is divided into three parts. The rightmost one contains the bulk of the

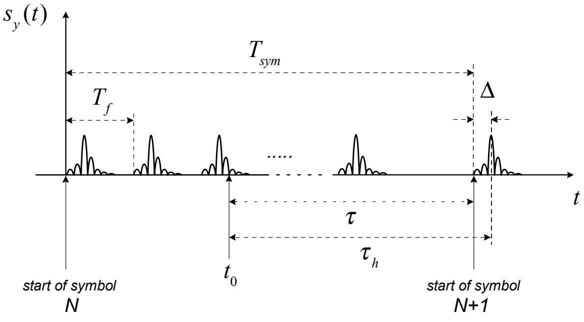


Fig. 4. Illustration of the pulses in symbol N

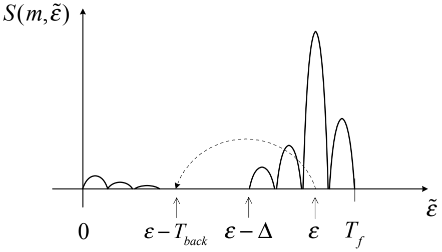


Fig. 5. Shape of $S(m, \tilde{\varepsilon})$ in the absence of noise

$q(t)$-pulse, with the possible exception of its right tail. The middle part is a noise-only-region (NOR). The leftmost portion supports the missing tail (if any) and is called *tail region*.

At first sight the following backward search [5] seems adequate to measure $\varDelta$. Starting from $\tilde{\varepsilon} = \varepsilon$ one goes backward by T_{back} to some point in NOR. Next, a rightward search is performed until $S(m, \tilde{\varepsilon})$ crosses some threshold λ, so indicating that the beginning of the $q(t)$-pulse has been reached. When this occurs, the distance to the highest peak gives the desired estimate $\hat{\varDelta}$ of $\varDelta$.

Unfortunately, large errors are incurred if the search starts in the tail region rather than in the NOR. In fact, when this happens, the threshold is likely to be crossed just at the beginning of the search. An expedient to reduce the risk is to modify $S(m, \tilde{\varepsilon})$ so as to eliminate the tail region. This goal is achieved bearing in mind that the tail arises from the presence of $q(t)$-pulses at a distance T_f in the received waveform. Thus, dropping the terms in (26) with index k such that $d^2_{|k-m|_{K_{pbs}}} = d^2_{|k-m-1|_{K_{pbs}}} = 1$ does the trick. As a result (26) becomes

$$\bar{S}(m, \tilde{\varepsilon}) \triangleq \frac{1}{K_s} \sum_{i=0}^{K_s-1} \sum_{k \in \mathcal{I}(m)} d^2_{|k-m|_{K_{pbs}}} s_y(t_0 + \tilde{\varepsilon} + T_k^j) \tag{27}$$

where $\mathcal{I}(m)$ is the set of indices k such that $d^2_{|k-m|_{K_{pbs}}} = 1$ and $d^2_{|k-m-1|_{K_{pbs}}} = 0$.

Some remarks are useful.

(a) As is done in the highest-peak search, it is convenient to proceed digitally and replace $\bar{S}(m, \tilde{\varepsilon})$ with its sampled version $\bar{S}(m, \tilde{n}T_s)$.

(b) A key design parameter not only here but also in the frequency domain estimator is the threshold value. If the threshold is small compared with the peaks, the crossing occurs before than it should and then we say that a false alarm has happened. Vice versa, if the threshold is large, the crossing occurs after than it should and the TOA is underestimated. By simulation we have found a satisfactory trade off for the value of the threshold.

5 Numerical Results

For numerical evaluation of the algorithm we consider the channel models developed within the framework of the IEEE 802.15.4a. In particular it is used the CM1 Residential LOS channel model. All simulations are given for 100 independent channel realizations. The main simulation parameters are shown in Table 1. The monocycle $p(t) = c(t)\cos(2\pi f_0 t)$ is a modulated 8th order Butterworth pulse with a 3dB bandwidth of 500 MHz and a center frequency $f_0 = 4.5$ GHz. Pulse $c(t)$ is compliant with channels 0:3, 5:6, 8:10 and 12:14 of the IEEE 802.15.4a Standard. The pulse repetition period is $T_f = T_{sym}/K_{pbs}$ =128 ns.

Fig. 6 depicts the root mean squared error (RMSE) of the estimated TOA of both estimators. Results show that an estimation accuracy of few centimeters is asymptotically achieved for high values of SNR with both estimators (13cm in frequency domain and 9.5cm in time domain). Although the time domain estimator seems to be slightly more accurate than the frequency domain estimator for high

Table 1. Simulation Parameters

Parameter	Value
Pulse duration $p(t)$, T_p	2 ns
Number of frames per symbol, PRF and K_{pbs}	31
Preamble SYNCH length, L_p and N_{SYNC}	1024 symbols
Number of symbols in the acquisition interval, K_s	974 symbols
Symbol duration, T_{sym}	3974.4 ns
Sampling rate, $1/T_s$	1 GHz

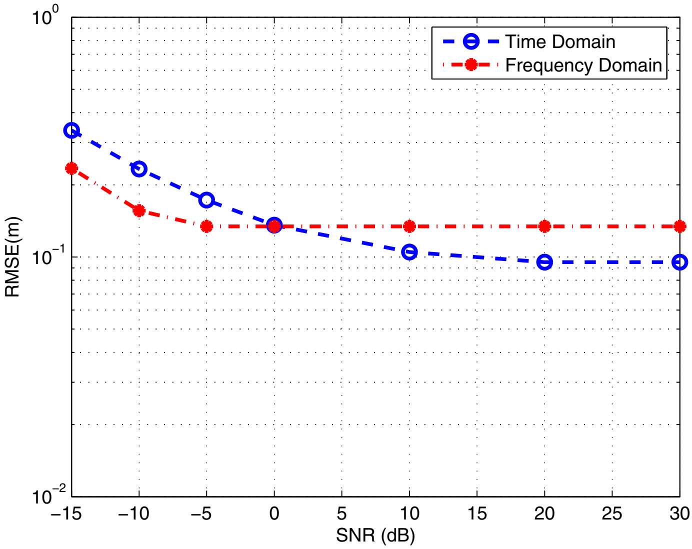


Fig. 6. RMSE(m) of the estimated TOA of both estimators vs. SNR

SNR, it can be observed that the curve corresponding to the frequency domain estimator grows slower as the SNR decreases than the curve corresponding to the time domain estimator.

6 Conclusion

A comparison between time and frequency domain TOA estimators has been made. The time domain algorithm looks for the ranging marker, i.e., the arrival time of the first pulse of the physical layer header. The goal is achieved in two steps: (a) determining the arrival time of the first pulse of each symbol in the preamble; (b) locating the exact position of the start frame delimiter. The frequency domain estimator exploits the low complexity of the FFT calculation by means of a power delay spectrum computation. The fine TOA estimatior requires a previous stage that provides a coarse symbols synchronization. It has been shown that time domain estimator works slightly better for high values of SNR while frequency domain estimator seems to provide more accurate results at low values of SNR.

References

1. D'Amico, A.A., Mengali, U., Taponecco, L.: Ranging Algorithm for the IEEE 802.15.4a Standard. In: Proceedings IEEE International Conference on Ultra-Wideband, September 9-11, pp. 285–289. IEEE, Vancouver (2009) ISBN 978-1-4244-2931-8
2. D'Amico, A.A., Mengali, U., Taponecco, L.: TOA Estimation with the IEEE 802.15.4a Standard. Submitted to the IEEE Transactions on Wireless Communications (April 15, 2009)
3. Navarro, M., Nájar, M.: Frequency Domain Joint TOA and DOA estimation in IR-UWB. Submitted for publication to the IEEE Trans. on Wireless Communications (October 2008) (under review)
4. Navarro, M., Nájar, M.: Joint estimation of TOA and DOA in IR-UWB. In: IEEE Workshop on Signal Processing Advances in Wireless Communications, Helsinki, Finland, June 17-20, pp. 1–5 (2007)
5. D'Amico, A.A., Mengali, U., Taponecco, L.: Energy-Based TOA Estimation. IEEE Trans. on Wireless Communications 7(3), 838–847 (2008)

Trade-off between Feedback Load for the Channel State Information and System Performance in MIMO Communications

Daniel Sacristán-Murga[1] and Antonio Pascual-Iserte[1,2,⋆]

[1] Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)
[2] Department of Signal Theory and Communications, Universitat Politècnica de Catalunya (UPC)
`daniel.sacristan@cttc.es, antonio.pascual@upc.edu`

Abstract. The performance of multiple-input multiple-output (MIMO) communication systems is greatly increased by having channel state information (CSI) at the transmitter. In systems with no channel reciprocity, a limited feedback link is used to send the CSI from the receiver to the transmitter. However, the resources for the feedback link come at the expense of resources from the communications link. This paper studies the trade-off between accurate feedback and system performance for systems using different feedback techniques. The optimum feedback load is computed for different transmission schemes including time-division duplex (TDD) and frequency-division duplexing (FDD).

Keywords: MIMO systems, feedback communication, quantization, limited feedback, multiuser systems.

1 Introduction

The use of multiple antennas at both the transmitter and the receiver is known to increase the performance of a communication system greatly, in terms of capacity [1] and resilience to fading [2]. In order to maximize this performance increase, complete knowledge of the propagation channel is required. This is easily obtained at the receiver by means of a training signal and channel estimation techniques. However, at the transmitter, this is not possible if channel reciprocity does not hold. In this scenario a dedicated feedback link can be used to send the required channel state information (CSI) from the receiver to the transmitter.

There has been extensive research on quantization and feedback techniques for transmitting the CSI from the receiver to the transmitter. However, in most

---

[⋆] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 248267 (BuNGee) and no. 216715 (NEWCOM++). It has received further support from the Catalan Government under grant 2009 SGR 891, and by the Spanish Government under project TEC2008-06327-C03 (MULTI-ADAPTIVE).

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 518–529, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

cases the performance analysis is evaluated without taking into account the cost of using feedback. If we take this cost into account explicitly it turns out that, while using a large amount of feedback improves the quality of the CSI available at the transmitter, it is not optimum from a perspective of system performance since the remaining radio resources available for the data link are lower. This is because the differential gain obtained by each additional feedback bit is a decreasing function and, eventually, it gets lower than the cost of dedicating an additional bit to feedback. In this paper we show that using low feedback rate is better than not using feedback at all and also better than using large amounts of feedback.

The paper is organized as follows. The system and signal models are given in section 2. Section 3 presents a review of available feedback strategies, and then the performance evaluation of the different techniques follows in section 4. Section 5 is devoted to the study of the trade-off between performance and allocation of radio resources between the data link and the feedback link. Finally, section 6 concludes the paper.

2 System and Signal Models

Let us consider a flat fading MIMO channel with n_T and n_R transmit and receive antennas, respectively, represented at time instant n by $\mathbf{H}(n) \in \mathbb{C}^{n_R \times n_T}$. The n_R received signals at the same time instant, assuming a linear transmitter, can be expressed as

$$\mathbf{y}(n) = \mathbf{H}(n)\mathbf{B}\left(\widehat{\mathbf{R}}_H(n)\right)\mathbf{x}(n) + \mathbf{w}(n) \in \mathbb{C}^{n_R}, \tag{1}$$

where $\mathbf{x}(n) \in \mathbb{C}^{n_S}$ represents the n_S streams of signals to be transmitted with $\mathbb{E}\left\{\mathbf{x}(n)\mathbf{x}^H(n)\right\} = \mathbf{I}$, and $\mathbf{B} \in \mathbb{C}^{n_T \times n_S}$ is the linear transmitter matrix that must satisfy the mean transmit power constraint $\|\mathbf{B}\|_F^2 \leq P_T$ ($\|\cdot\|_F$ stands for the Frobenius norm). Note that we explicitly indicate that the transmitter depends on the available estimate of the channel Gram matrix $\widehat{\mathbf{R}}_H(n)$, where the exact matrix is $\mathbf{R}_H(n) = \mathbf{H}^H(n)\mathbf{H}(n)$ (the optimum precoding matrix $\mathbf{B}$ depends only on $\mathbf{R}_H(n)$ as proved in [3], [4]). The additive white Gaussian noise (AWGN) at the receiver is represented by $\mathbf{w}(n) \in \mathbb{C}^{n_R}$ with $\mathbb{E}\big\{\mathbf{w}(n)\mathbf{w}^H(n)\big\} = \sigma_w^2\mathbf{I}$.

As a performance criterion we consider the packet transmission rate and also the mutual information using a Gaussian code, which is expressed as $\log_2 \det\left(\mathbf{I} + \frac{1}{\sigma_w^2}\mathbf{B}\mathbf{B}^H\mathbf{R}_H\right)$, as will be explained later in section 5.

3 Review of Feedback Strategies

Since the performance of the transmission scheme with partial CSIT depends on the feedback strategy followed, we will briefly introduce the feedback techniques evaluated in this paper. We will consider both non-differential and differential types of feedback [5], [6].

3.1 Non-differential Feedback

The non-differential algorithms are based on the quantization of the CSI using a codebook, which is a set of precoding matrices that is known to the transmitter and the receiver. The receiver evaluates the performance for all the elements (codewords) in the set, and sends to the transmitter the index of the codeword that provides the best performance given the current channel. The main advantage of this technique is its simplicity, while its main drawback is that it does not exploit the correlation in time present in most real channels. There are different techniques to generate the codebook, such as the ones based on packaging in the Grassmannian manifold [7] or iterative procedures like in [5]. The techniques described in these references perform a quantization of the subspaces that correspond to the right eigenvectors of the channel matrix and do not consider the information of the individual eigenvalues. Consequently, the power allocation between spatial modes is constrained to be uniformly distributed.

3.2 Differential Feedback

A differential feedback strategy is based on a quantization of the difference between the last known value of CSI and the current value. Only the information related to the update in the CSI is fed back to the transmitter, and this improves greatly the performance in time correlated channels at the cost of some slight complexity increase. In this paper we will evaluate the differential algorithm explained in detail in [6]. This algorithm performs a quantization of the channel Gram matrix ($\mathbf{R}_H = \mathbf{H}^H\mathbf{H}$), which is an Hermitian positive definite matrix by construction. The set of Hermitian positive definite matrices has the geometry of a convex cone [8], and this technique exploits such geometry. The algorithm is composed of 3 steps, which are performed at every feedback update. As depicted in Fig. 1, the steps for feedback interval n are defined as:

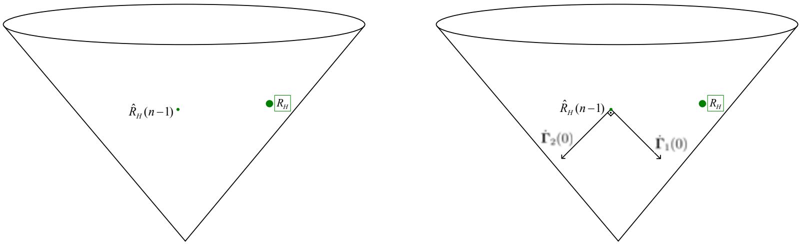
- ***Initial situation:*** The receiver has a perfect knowledge of the current channel matrix $\mathbf{H}(n)$. Both the transmitter and the receiver know which is the last quantization of the channel Gram matrix sent through the feedback channel $\widehat{\mathbf{R}}_H(n-1)$. At the first feedback transmission the algorithm starts from the cone vertex: $\widehat{\mathbf{R}}_H(0) = \mathbf{I}$ (Fig. 1.a).
- ***Step 1:*** Both the receiver and the transmitter generate a common set of Q geodesic curves[1] $\mathbf{\Gamma}_i(t)$ $(i = 1 \ldots Q)$ on the cone, having all of them the same initial point and with orthogonal directions[2] $\dot{\mathbf{\Gamma}}_i(t)\Big|_{t=0}$, which are determined by the $\mathbf{C}_i$ matrices[3] (Fig. 1.b,c).

---

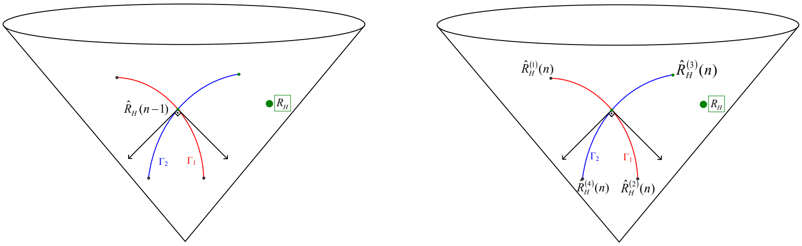
[1] A geodesic curve is defined as the path connecting two points in the set with minimum distance and with all its points belonging to the set. Consequently, its expression depends on the geometry of the set.

[2] The maximum number of orthogonal directions is given by the dimension of the set of Hermitian matrices, i.e., $Q \leq n_T^2$. If the number of feedback bits is higher than $\log_2(2n_T^2)$, the additional directions will have the orthogonality constraint relaxed.

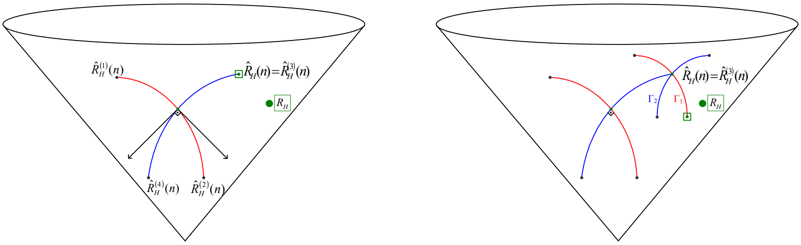
[3] The quantization step is related to the norm of $\mathbf{C}_i$ and can be optimized for any scenario and mobility conditions.



(a) Initial situation (b) Step 1



(c) Step 1 (d) Step 2



(e) Step 3 (f) Next time instant

Fig. 1. Example of one feedback computation in a 2-bit differential quantization, using as optimization criterion the minimization of the geodesic distance to the actual channel Gram matrix $\mathbf{R}_H$

$$\mathbf{\Gamma}_i(t) = \widehat{\mathbf{R}}_H^{1/2}(n-1)\exp\left(t\mathbf{C}_i\right)\widehat{\mathbf{R}}_H^{1/2}(n-1). \tag{2}$$

- ***Step 2:*** Each of these geodesic curves $\mathbf{\Gamma}_i(t)$ is used to generate two candidates ($\mathbf{\Gamma}_i(1)$ and $\mathbf{\Gamma}_i(-1)$) for the feedback in the next iteration (Fig. 1.d).
- ***Step 3:*** The receiver evaluates the cost function for each of the candidates, selects the candidate that minimizes the cost function and sends the corresponding index i_{FB} through the feedback channel to the transmitter (Fig. 1.e). The selected matrix will be used for the transmitter design and as the starting point in the next feedback computation (Fig. 1.f).

4 Effect of Feedback on the Performance

This section will characterize, from a simulations perspective, the performance improvement achieved using the differential and non-differential feedback techniques described in section 3.

We consider a random MIMO channel following a first-order autoregressive time variation model, which is described by the expression:

$$\mathbf{H}(n) = \rho\mathbf{H}(n-1) + \sqrt{1-\rho^2}\,\mathbf{N}(n), \tag{3}$$

where matrices $\mathbf{H}(0)$ and $\mathbf{N}(n)$ are assumed to be independent and composed of i.i.d. zero-mean complex Gaussian entries with unit variance. The time correlation factor ρ models the variability of the channel and depends on the Doppler frequency f_D caused by the movement of the transmitter/receiver through the expression $\rho = J_0\big(2\pi f_D \tau\big)$ [9], where J_0 is the zeroth-order Bessel function of the first kind and τ corresponds to the time difference between consecutive feedback instants. Note that the case of an invariant channel corresponds to $\rho = 1$. The time correlation factor is usually expressed in the literature in terms of the normalized Doppler frequency $f_D\tau$, or f_D/f_{FB}, where f_{FB} is the frequency of feedback messages. The values for this parameter usually considered in the literature are $0.004 < f_D/f_{FB} < 0.01$ (see references [10,11,12]), which correspond to $0.999 < \rho < 1$.

Fig. 2 shows the performance in terms of mutual information in a system with $n_T = 3$, $n_R = 3$, a normalized Doppler frequency of $f_D/f_{FB} = 0.05$ and a transmitted power of 0.5W. The simulations are averaged over 1000 channel

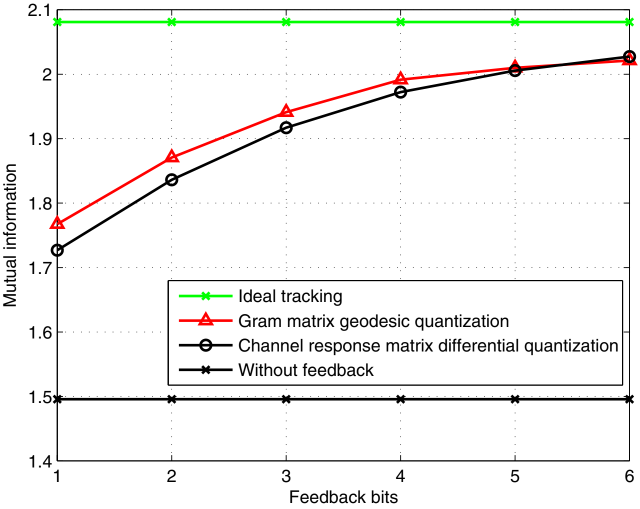


Fig. 2. Mutual information in a 3 × 3 channel with $P_{tx} = 0.5, f_D/f_{FB} = 0.05$

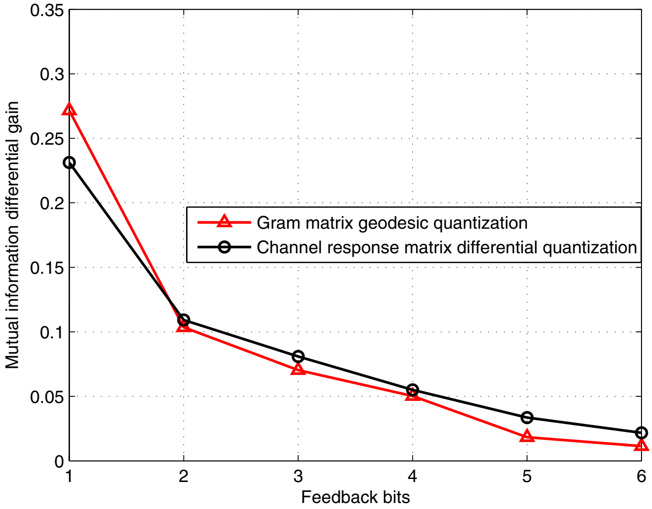


Fig. 3. Differential gain in mutual information in a 3 × 3 channel with $P_{tx} = 0.5, f_D/f_{FB} = 0.05$

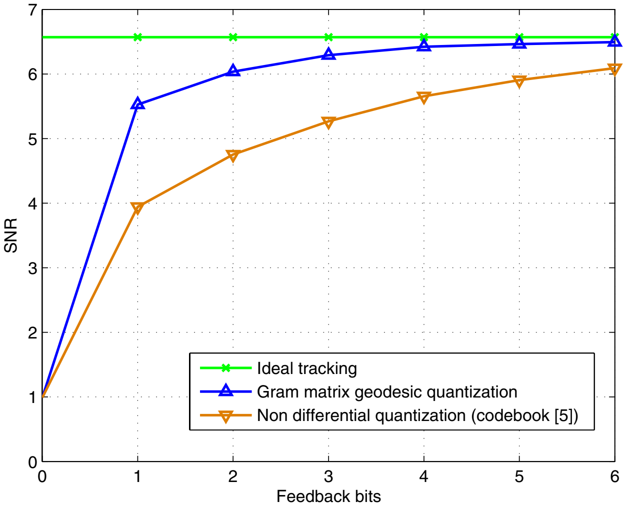


Fig. 4. SNR versus the number of feedback bits

realizations and show an improvement in the mutual information of 20% using just one bit of feedback, and up to more than 50% in the case of 6 bits of feedback. The incremental gain obtained by the use of each additional feedback bit

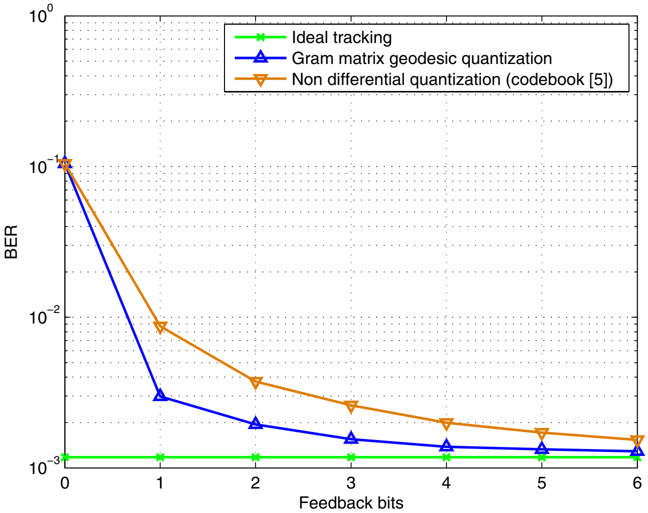


Fig. 5. BER versus the number of feedback bits

is plotted in Fig. 3. It is a decreasing function, which means that the first bit introduces a great gain and each successive bit used provides a smaller gain. In these figures the differential feedback algorithm from [6] is compared to a differential quantization algorithm applied directly to the channel response matrix $\mathbf{H}$ of the system instead of $\mathbf{R}_H$ (so, the geometry of the convex cone corresponding to $\mathbf{R}_H$ is not exploited).

The performance in terms of SNR is shown in Fig. 4, considering the following setup: $n_T = 3$, $n_R = 3$, $f_D/f_{FB} = 0.03$ and a transmitted power of 1W. The simulations are averaged over 1000 channel realizations and show a performance that increases with the number of bits of feedback. The differential strategy provides a better result than the non-differential one because it exploits the temporal correlation of the channel.

Fig. 5 considers the same scenario, but studies the bit-error-rate (BER) using a BPSK modulation. The curves show a large improvement in the BER when using feedback and in this case the differential scheme also outperforms the quantization based on codebooks because it exploits the correlation in time of the channel.

5 Resource Allocation between Data and Feedback Transmission

In section 4, we have evaluated the benefits of having CSI at the transmitter. In this section we will introduce in the system a variable for the cost of using feedback, in order to study the tradeoff between achievable communication performance and radio resource allocation between the feedback and the data link. In the case of time-division duplex (TDD), the resource that is shared between data and feedback link corresponds to the transmission time, whereas in frequency-division duplexing (FDD) the resource to be shared is the bandwidth. We will now see that to the purpose of resource allocation both schemes are dual, and we will optimize the resource allocation for the general case.

5.1 TDD and FDD Systems

In systems where different information streams share the same physical communications link, the available link resources have to be shared. In the case considered in this paper the data and feedback information share the pool of radio resources. We will consider two duplexing schemes: dividing the time axis in different time slots and assigning each slot to the transmission of either data or feedback information (TDD), and dividing the frequency axis in different bandwidth slots, corresponding to feedback or data transmission (FDD). For the equations describing these schemes we use the following notation:

- W_t: total available bandwidth.
- W_d: bandwidth dedicated to transmission of data.
- $W_f = W_t - W_d$: bandwidth dedicated to transmission of feedback.
- T_t: total duration of a time frame.
- T_d: time dedicated to transmission of data.
- $T_f = T_t - T_d$: time dedicated to transmission of feedback.
- E_t: total available energy for the transmission of data.
- N_0: noise power spectral density (AWGN).
- R_d: rate at which data can be transmitted.
- $\mathbf{H} \in \mathbb{C}^{n_R \times n_T}$: flat fading MIMO channel with n_T and n_R transmit and receive antennas, respectively
- $\mathbf{B}(n) \in \mathbb{C}^{n_T \times n_S}$: linear transmitter matrix that satisfies $\|\mathbf{B}\|_F^2 \leq 1$.

Frequency-division duplex. The FDD scheme features continuous transmission of data and feedback simultaneously, by dividing the total bandwidth available W_t between the data and the feedback link, as depicted in Fig. 6.

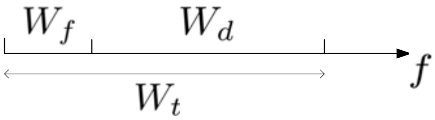


Fig. 6. FDD system model

In such a system, the maximum achievable data rate is given by the following expression, which is an increasing function of the available bandwidth W_d:

$$R_d = W_d \log_2 \det \left(\mathbf{I} + \frac{\frac{E_t}{T_t}}{W_d N_0} \mathbf{H}^H \mathbf{H} \mathbf{B} \mathbf{B}^H \right) \quad \text{(bits/s)}. \tag{4}$$

Time-division duplex. On the other hand, the TDD scheme makes use of the complete bandwidth to transmit either data or feedback information[4]. The scheduling is performed in the time domain, i.e., there are time slots where all the bandwidth is devoted to sending data and in the other time slots all the bandwidth is dedicated to the feedback link, as depicted in Fig. 7

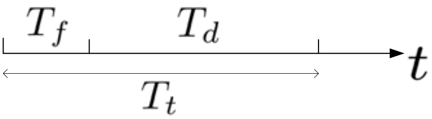


Fig. 7. TDD system model

In a TDD system, the maximum achievable data rate is an increasing function of the time devoted to transmitting data, and is given by the following expression:

$$R_d = \frac{T_d}{T_t} W_t \log_2 \det \left(\mathbf{I} + \frac{\frac{E_t}{T_d}}{W_t N_0} \mathbf{H}^H \mathbf{H} \mathbf{B} \mathbf{B}^H \right) \quad \text{(bits/s)} \qquad (5)$$

General expression (TDD + FDD). As observed in (4) and (5), the expressions of the data rate for both TDD and FDD are dual, and they behave exactly the same as a function of variables T_d and W_d, respectively. It is possible to jointly formulate this dependance (based on (4) and (5)):

$$R_d = \frac{T_d}{T_t} \frac{W_d}{W_t} W_t \log_2 \det \left(\mathbf{I} + \frac{E_t}{T_t W_t N_0} \frac{1}{\frac{T_d}{T_t} \frac{W_d}{W_t}} \mathbf{H}^H \mathbf{H} \mathbf{B} \mathbf{B}^H \right) \quad \text{(bits/s)} \qquad (6)$$

The case where $T_d = T_t$ corresponds to FDD, and $W_d = W_t$ corresponds to TDD.

Expression (6), normalized to the bandwidth, can also be written as:

$$R_d = \alpha \log_2 \det \left(\mathbf{I} + \frac{snr}{\alpha} \mathbf{H}^H \mathbf{H} \mathbf{B} \mathbf{B}^H \right) \quad \text{(bits/s)}, \qquad (7)$$

where $\alpha = \frac{T_d}{T_t} \frac{W_d}{W_t}$ $(0 \leq \alpha \leq 1)$ and $snr = \frac{E_t}{T_t W_t N_0}$.

Following (7), the optimum allocation of resources for data and feedback transmissions can be performed. Fig. 8 shows the results for the case of a 3×3 channel

---

[4] In the literature it is usually assumed that in TDD systems there is channel reciprocity and therefore feedback is not required. In practical systems, however, the radio frequency (RF) chains have a different response for transmission and for reception. There are two solutions to this issue: one option is to do feedback of the CSI (which includes obviously the effect of the RF chain) and the other option is to perform a calibration of the RF chains for transmission and for reception. In this paper only the feedback solution is considered.

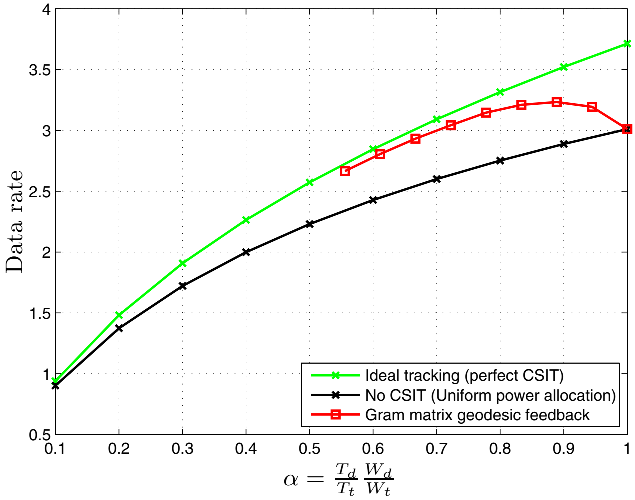


Fig. 8. Data rate versus time dedicated to data and feedback transmission

and a normalized doppler frequency of $f_D/f_B = 0.05$. In this simulation it was considered that each bit of feedback used required 1/18 of the available resources in order to obtain an error-free feedback transmission. These results show that, for this particular setup, the largest data rate is achieved by using 2 bits of feedback, i.e. assigning 2/18 of the resources to the feedback link and the remaining 16/18 to the data link.

5.2 A Practical Case

In this section we study a practical situation of single beamforming, featuring the transmission of frames with a fixed length of 18 bits. 2 of these bits are reserved for control and other information. Of the remaining $L = 16$ bits, N of them are used for feedback and the rest $(L - N)$ are used for data transmission, as depicted in Fig. 9.

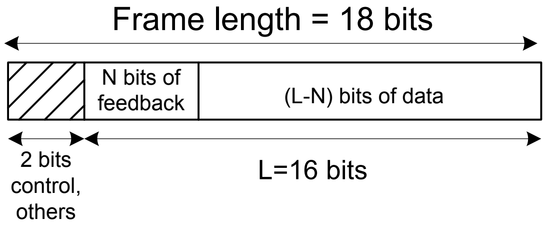


Fig. 9. Frame structure

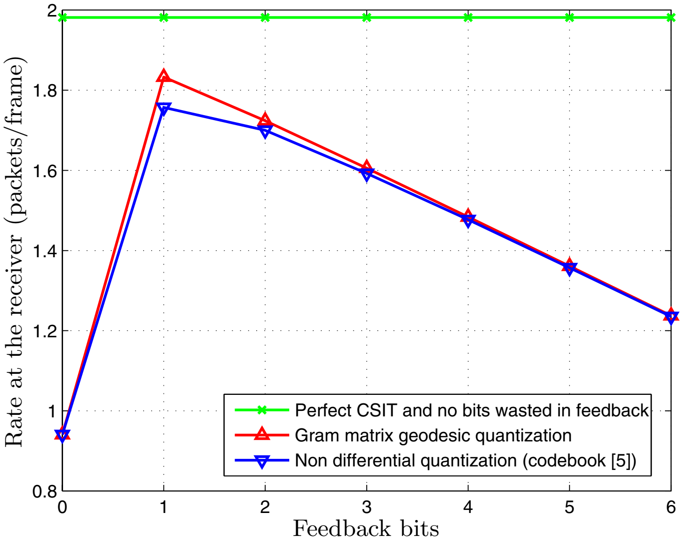


Fig. 10. Average number of data packets received correctly for each frame

We now consider the optimum allocation of bits between the feedback and data links. Note that the transmission of feedback is done through a noise-free and delay-free link, and the transmission of data is done using a QPSK modulation in AWGN.

The data is transmitted in packets of L_p bits. We assume that if there is a transmission error in one of the bits of the packet, the packet is discarded. This means that on average for each frame the number of packets received without errors is:

$$\frac{L-N}{L_p}(1-PER)=\frac{L-N}{L_p}(1-BER)^{L_p}\,. \tag{8}$$

Following this expression, Fig. 10 shows the packet rate per frame for the case of $P_{tx}=1$, $L=16$, $L_p=8$ and a 3×3 MIMO time variant channel with normalized Doppler of $f_D/f_{FB}=0.05$. The results are averaged over 1000 channel realizations. The resulting curves show that, for the scenario considered, the best packet transmission rate is achieved when using a feedback load of 1 bit. This holds for the differential and also the non-differential feedback schemes.

6 Conclusions

This work presented an analysis of the resource allocation (time and bandwidth) between the data and the feedback link of a MIMO communication system. It is shown that, since resources for the feedback transmission come at a cost of resources for the data transmission, there is an optimum resource allocation strategy that maximizes system throughput.

We considered non-differential and differential feedback algorithms, with special focus on the later, and performed simulations for different scenarios. The results show that a low rate feedback link is usually enough to provide almost all CSI to the transmitter, and the additional accuracy obtained by increasing the feedback load does not compensate for the loss in bits that would otherwise be used to transmit data.

References

1. Telatar, I.E.: Capacity of multi-antenna Gaussian channels. European Trans. on Telecommunications 10(6), 585–595 (1999)
2. Alamouti, S.M.: A simple transmit diversity technique for wireless communications. IEEE Journal on Selected Areas in Communications 16(8), 1451–1458 (1998)
3. Payaró, M., Palomar, P.: On optimal precoding in linear vector Gaussian channels with arbitrary input distribution. In: IEEE International Symposium on Information Theory (ISIT 2009), Seoul (2009)
4. Palomar, D.P., Cioffi, J.M., Lagunas, M.A.: Joint Tx-Rx beamforming design for multicarrier MIMO channels: a unified framework for convex optimization. IEEE Transactions on Signal Processing 51(9), 2381–2401 (2003)
5. Roh, J.C., Rao, B.D.: Design and analysis of MIMO spatial multiplexing systems with quantized feedback. IEEE Transactions on Signal Processing 54(8), 2874–2886 (2006)
6. Sacristán-Murga, D., Pascual-Iserte, A.: Differential feedback of MIMO channel correlation matrices based on geodesic curves. In: 34th IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2009), Taipei (2009)
7. Love, D.J., Heath, R.W., Strohmer, T.: Grassmannian beamforming for multiple-input multiple-output wireless systems. IEEE Transactions on Information Theory 49(10), 2735–2747 (2003)
8. Talih, M.: Geodesic Markov chains on covariance matrices. In: Statistical and Applied Mathematical Sciences Institute, pp. 1–27 (2007)
9. Steele, R., Hanzo, L.: Mobile Radio Communications. John Wiley & Sons, Chichester (1999)
10. Yang, J., Williams, D.B.: Transmission subspace tracking for MIMO systems with low-rate feedback. IEEE Transactions on Communications 55(8), 1629–1639 (2007)
11. Inoue, T., Heath, R.W.: Geodesic prediction for limited feedback multiuser MIMO systems in temporally correlated channels. In: 4th IEEE Radio and Wireless Symposium, San Diego (2009)
12. Roh, J.C., Rao, B.D.: Efficient feedback methods for MIMO channels based on parameterization. IEEE Transactions on Wireless Communications 6(1), 282–292 (2007)

Evolution of Spatial and Multicarrier Scheduling: Towards Multi-cell Scenario

Pol Henarejos[1,⋆], Ana Perez-Neira[1,2], Velio Tralli[3], Marco Moretti[4],
Nikos Dimitriou[5], and Giulio Dainelli[5]

[1]Centre Tecnòlogic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain
`pol.henarejos,ana.perez@cttc.es`
[2]Universitat Politècnica de Catalunya (UPC), Barcelona, Spain
[3]CNIT, University of Ferrara, Ferrara, Italy
`velio.tralli@unife.it`
[4]Dipartimento di Ingegneria dell'Informazione, Universita di Pisa, Italy
`marco.moretti@iet.unipi.it`
[5]Institute of Acelerating Systems & Applications, National Kapodistrian University
of Athens, Athens, Greece
`nikodim@phys.uoa.gr`

Abstract. OFDMA systems are considered as the promising multiple access scheme of next generation multi-cellular wireless systems. In order to ensure the optimum usage of radio resources, OFDMA radio resource management algorithms have to maximize the allocated power and rate of the different subchannels to the users taking also into account the generated co-channel interference between neighboring cells, which affects the received Quality of Service. This paper discusses various schemes for power distribution schemes in multiple co-channel cells. These schemes include centralized and distributed solutions, which may involve various degrees of complexity and related overhead and may employ procedures such as linear programming. Finally, the paper introduces a new solution that uses a network flow model to solve the maximization of the multi-cell system sum rate. The application of spatial beamforming at each cell is suggested in order to better cope with interference.

1 Introduction

Most of the existing literature on resource allocation focuses on the single cell scenario, where all users are assigned to a different portion of the available spectrum. However, mobile communication systems are better described as multi-cellular systems where either coordinated or uncoordinated cells transmit on the same bandwidth and are therefore the capacity is increased, but not unaffected by Multiple Access Interference (MAI). MAI in particular deteriorates the performance of users near cell boundaries. Thus, any resource allocation problem in

---

[⋆] This work was supported by the European Commission under the Network of Excellence NEWCOM++ (216715). The authors thank the partners of WPR8 in Newcom++ NoE for their valuable technical help.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 530–542, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

a multi-cell environment has to take into account the impact of the MAI on the system. A frequency reuse factor larger than one guarantees a large reduction of the interference at the cost of a reduction of the efficiency in the usage of spectral resources. For this reason in recent literature several works have focused on Orthogonal Frequency Division Multiple Access (OFDMA) allocation in multicarrier cellular systems with a frequency reuse factor equal to one. Due to the strong impact of MAI in this scenario, it is important to take full advantage of frequency and multi-user diversity of the system. The authors from [1] set the initial point to start the current research, in which is addressed this manuscript.

In the past years, several approaches relying on the concept of inter-cell coordination have emerged, which can be distinguished in two categories: packet-based coordination and resource-allocation based coordination. In the first one, data packets destined to the users are replicated at several base stations, before jointly precoding/beamforming, and transmitting from all the Base Station antennas (BS) [2], [3], [4]. The drawback of this approach is a large overhead in inter-cell signaling, packet routing, and feedback for exchanging the channel state information required to compute the precoders. In the second approach, the interference is tackled by means of coordinated resource control (power, scheduling, etc.) between the cells [5], [6] which make lower complexity and distributed coordination techniques are possible. Power control and smart soft reuse partitioning are possible strategies that can be applied [7], [8], [9].

Dynamic multi-cell power control targeted at maximizing the sum of user rates in the network is a very difficult task and does not lend itself easily to a distributed (across the cells) implementation, except for some particular cases with a large number of users [10]. The reason is as follows: dynamic power control affects the Signal to Interference plus Noise Ratio (SINR) of all users in all cells in a fully coupled manner making interference unpredictable.

OFDMA resource allocation is a viable solution to exploit channel and multi-user diversity in wireless communication systems. In a multi-user scenario, with an OFDMA multiple access scheme, each user is assigned a subset of orthogonal subcarriers. If the transmitter has full knowledge of the Channel State Information (CSI), subcarriers can be assigned with the goal of maximizing some optimality criterion. Since the radio propagation channels are statistically independent among the users, what is a bad channel for one user may be a good one for another and thus, thanks to the effect of multi-user diversity, dynamic resource allocation largely increases the system spectral efficiency.

Resource Allocation schemes in a multi-cell scenario can be divided into centralized and distributed algorithms. Centralized schemes perform allocation through a central unit like the Radio Network Controller (RNC) that collects CSI and interference level for each user in the system. Ideally, the RNC decides which subchannels (or subcarriers) to assign to each single user with the suitable format and power level. On the other hand, in a distributed algorithm resource allocation is performed autonomously by each single BS in its cell. The main problem for centralized schemes is the large amount of signaling needed for exchanging CSI and allocation feedback. Moreover, the allocation complexity grows exponentially with the number of users in the network, since resource assignment is realized by a single unit, which has to process large amounts of data. Thus, centralized algorithms are often studied to provide an ideal bound for the performance of others schemes. Distributed algorithms require lower complexity and signaling, since they perform allocation locally at each BS and therefore require only the information about the users in the cell. However, such solutions very often lead to iterative algorithms, which may have convergence problems. Sometimes the differences between distributed and centralized schemes blur away since distributed schemes may require a limited amount of centralized information to improve their performance.

Recently, the spatial diversity has been introduced to reach an acceptable performance. Many solutions of the current State of Art (SoA) propose Multiple Input Multiple Output (MIMO) techniques, widely extended for the single cell scenarios. Nevertheless, these schemes treat inter-cell interference as noise, where the performance is limited, specially for edge-cell users. The authors in [11], [12] and [13] deal with this kind of problem. Unfortunately, computational power and complexity raise up with the number of cells. Thus, distribution forms of cooperation among the user terminals and BS appear with great interest. One alternative is cooperative MIMO to minimize total power with QoS constraints [14]. This scheme implies that BS are going to change their peak power and may be not suitable in several scenarios. This manuscript present a second alternative of cooperative MIMO to maximize a cost function of rate. If the cost function is the sum rate function, the problem becomes NP-hard [15]. However, other cost functions are possible to decrease its complexity [16].

This document aims to organize the SoA according to the requirements of the system, if the interference management is relevant or not. Moreover, two algorithms to distribute users in the several cells and power allocation are also presented. Thereby, section 2 introduces the different techniques used in the OFDMA power distribution in multi-cell scenarios. Section 3 presents a scheme to distribute users in the several cells, with centralized or distributed complexity, based on the Linear Programming (LP). Furthermore, section 4 describes a framework to perform the power allocation and user selection from the approach of a single-cell multi-antenna scenario. Finally, this document is ended by the conclusions.

2 Power Distribution for OFDMA Multi-cell Systems

Power has an important role in multi-cell systems not only for the rate optimization, but for the interference management. Networks where interference is not a big problem (such as those where there is frequency planning and adjacent cells use different OFDMA subcarriers) may strive to optimize the throughput. On the contrary, in networks where interference plays an important aspect, power strategy may be oriented to limit this interference. The following algorithms cover both categories.

2.1 Layered and Distributed Dynamic Resource Allocation Algorithm

A downlink communication system in a cellular network, where all cells adopt a frequency reuse factor equal to one, is considered. Each user CSI and the level of interference on each subcarrier are assumed to be perfectly known by each BS. Since in each cell a subchannel is allocated to at most one user, the effects of MAI depend on the users (and specifically on their location and power/rate allocation) that are allocated the same channel in adjacent cells. The MAI on channel m affecting user k in cell q is:

$$I_{k,m,q} = \sum_{j=1,j\neq q}^{Q} p_{m,q} G_{k,m,j} \tag{1}$$

where $p_{m,q}$ indicates the power transmitted by cell q on subcarrier m and $G_{k,m,j} = |h_{k,m,q}|^2$ is the channel gain between user k and cell q on subchannel m. Thus, the power required for achieving a certain target SINR is:

$$p_{k,m,q} = SINR \frac{BN_0 + I_{k,m,q}}{G_{k,m,q}} \tag{2}$$

where B stands for the bandwidth of the signal and N_0 is the noise power in W/Hz.

A layered architecture that integrates in each cell a Packet Scheduler (PS) with an adaptive resource allocator (RA) is considered. First, the RA allocates the resources with the goal of minimizing the transmitted power in each cell subject to user's rate constraints to keep low the MAI. To exploit multi-user diversity, the RA tends to assign most of the resources to the users that have good channel condition.

Second, the PS enforces long-term fairness in order to compensate the short term displacement of resources due to the RA. Moreover, a load control mechanism is introduced to force the convergence of the allocation. To reduce the complexity of the allocation phase, all users adopt only one transmission format with spectral efficiency η_0 for all the subcarriers so that rate constraints are translated into a number of resources, i.e., $R_{k,q} = B\eta_0 m_{k,q}$, where $m_{k,q}$ stands for the number of channels allocated to user k at cell q. The cost of a resource for a given user is the power required for achieving spectral efficiency η_0.

Whenever a cell modifies its allocation, it changes also the interference experienced by users in neighboring cells, which in turn change their allocation. Thus, the allocation phase is iterated until a stable allocation is reached in all cells. To help convergence, if the system is not able to reach a stable allocation, the load is progressively reduced in all cells.

After a stable allocation is reached, the PS updates the maximum rate requirements $m_{k,q}$ for each user in each cell with the goal of achieving long-term fairness. The convergence is not always guaranteed but the combined actions of load control and packet scheduling push towards convergence and fairness at the same time. An additional action to ensure convergence is provided by a mechanism where the most power consuming users can be progressively switched off. This approach tends to be unfair because users near the cell boundary risk to be too penalized in terms of the reduction of the available bandwidth. If not carefully designed, the main drawback of this scheme is the number of iterations required for achieving a stable allocation.

Minimum feedback layered and distributed dynamic resource allocation algorithm. A minimum feedback scheduling technique extends the concepts of distributed allocation that was outlined in the previous Section. It is assumed that each user measures the interference of each subcarrier and sends to the BS only the interference values that correspond to the “best” subcarriers. The number of those “best” subcarriers, i.e. those which experience the lowest MAI, is a parameter to be determined by the system operator. For the other subcarriers, the RA algorithm assumes the worst case scenario and assigns to them a fixed high value of interference. With this approach the required feedback is reduced while the RA algorithm has still the necessary inputs in order to be able to provide results. Of course, in this case the allocations will not be the optimal since the algorithm is forced to work without the actual interference values for all the subcarriers. However, it can be argued that it may provide similar throughput results as the previous algorithm with much less overhead and complexity [17].

Random subcarrier allocation algorithm. Another possible way to allocate resources to the users consists of a random resource allocation to the users in each cell, without any kind of optimization criteria. In this case the PS sets again the maximum number of subcarriers which can be assigned to the users, and then the allocator assigns randomly the subcarriers with respect to the constraints set by the PS. In this case, after random allocation, only power control takes place and after that the subcarriers which have not achieved their SINR target are switched off.

Additionally, users in the outer region of a cell will use a portion of the bandwidth which is different from that one utilized by the users in the outer region of the adjacent cells.

2.2 Power Planning

The objective is to achieve a fully distributed implementation of resource allocation over a multi-cell OFDMA network, whose aim is minimizing the network outage capacity. To reach this goal, the selection of the user to be scheduled and of the resources (here defined as the couple subcarrier/transmit power level) to be assigned to him, should be performed taking into account the channel gain and the received interference power. If a fully distributed approach is pursued, each BS can only rely on local information provided via a feedback channel by its own set of users. So, in this work some structuring inside the system is introduced, in order to make interference level inside the network predictable.

Though in principle power levels can continuously vary inside a predefined range, only a certain set of possible power levels are assumed, and these are distributed among cells and subcarriers according to a predefined pattern. This concept will be denoted from now on as “power planning”.

In particular, the network is organized in groups of Q adjacent cells according to a regular pattern as done for frequency planning in 2G systems and, for analogy, this group of cells is denoted as “cluster”. Then, the M equally spaced OFDMA subcarriers assigned to each cell are arranged in Q groups of M/Q adjacent subcarriers, from now on denoted also as “sub-bands”. It is clear that the larger the value of Q , the smaller the frequency diversity if correlation between subcarriers is taken into account.

A power vector $\mathbf{P} = [p_1 \dots p_Q]$ is introduced, which is composed of the Q power levels, also denoted as elements of the “power profile”. Hence, in the allocation process only these Q power values are usable. From now on, this vector will be denoted as “multi-cell transmit power vector”. Thus, the terms “power profile” and “multi-cell transmit power vector” are considered to represent identical things.

In each cell, every sub-band is assigned with one of the values belonging to power vector $\mathbf{P}$, and over all sub-bands inside a cell all values of $\mathbf{P}$ are exploited. Nevertheless, looking at a specific sub-band, the set of cells belonging to the same cluster use all power levels available in $\mathbf{P}$.

So, each cell in the network is assigned with a tag j ranging from 1 to Q denoting the cell type. Then, since each tag is assigned with a specific power vector (i.e., with a specific order of the possible Q power levels in vector $\mathbf{P}$), cells with the same tag will be assigned with the same power vector, whereas cells belonging to the same cluster are assigned with permutations of the original power vector.

3 Multi-cell User Assignment

Previous section was addressed to manage the power budget and choose which strategy can result more effective. However, this aspect also separates the power variable from the others. One of the advantages of decoupling the power variable depending on scenario requirements is the fact that users can be scheduled a posteriori following the same requirements. Even though the power can be used to schedule users, i.e. power equal to zero implies no user is scheduled, LP methods has been considered to be an efficient tool to solve this kind of problems. On the contrary, since power and user scheduling is performed in separated steps, solution becomes suboptimal.

Authors in [18] present a resource allocator for the uplink of multi-cell OFDMA systems. That concept is also applicable for the downlink channel. Previous section has defined the power strategy and power is solved in this point. Hence, user scheduling can be performed through LP. Even though authors in [18] minimize the power, the maximization of sum rate can also be pursued. Moreover, LP offers the chance to introduce more variables to the problem to make it as so general as it is desired.

Consider a downlink OFDMA system with Q cells with one BS each, K users distributed over all cells and M carriers available in each BS. Since power is defined in the previous sections, all rates of users are pre-defined in the following manner. The rate of kth user at mth carrier and qth cell is:

$$r_{k,m,q} = \log\left(1 + \frac{G_{k,m,q}p_{m,q}}{\sum_{q' \neq q}^{Q} G_{k,m,q'}p_{m,q'} + BN_0}\right) \tag{3}$$

where $p_{m,q}$ is the power served by qth cell at carrier m, defined previously.

This scheme can be easily combined with beamforming to decrease the effect of the interference. Thus, the BS may use a beam to increase the SINR and the overall sum rate.

3.1 Centralized Algorithm

A centralized approach could be done by modeling the multi-cell system as a single network with one central control unit which computes the access parameters for all users in all cells and the way with which users are scheduled over the network. In order to assign users to cells and carriers, LP algorithms are used and they prove to be a good way to exploit this kind of scenarios.

The problem can be stated as:

$$\begin{aligned} \mathbf{b} &= \arg\max_{\mathbf{b}} \sum_{q=1}^{Q}\sum_{k=1}^{K}\sum_{m=1}^{M} b_{k,m,q}r_{k,m,q} \\ s.t. &\sum_{k=1}^{K} b_{k,m,q} \leq 1,\ q = 1,\ldots,Q,\ m = 1,\ldots,M \\ &\sum_{q=1}^{Q} b_{k,m,q} \leq 1,\ k = 1,\ldots,K,\ m = 1,\ldots,M \end{aligned} \tag{4}$$

where $b_{k,m,q} = 1$ if user k is scheduled at mth carrier and in the qth cell and 0 otherwise. The first constraint implies that only one user can be scheduled in each carrier and cell. The second constraint, implies that only one cell can be assigned to one user at same carrier. This problem can be solved by LP easily. However, it requires centralized schemes and feedback corresponding to all $h_{k,m,q}$ that must be known at the transmitters. Although complexity is proportional to each variable that is introduced, results are near optimal.

3.2 Distributed Algorithm

The centralized algorithm is optimal compared to the distributed algorithm since it has more information about the channels of all users in all cells. On the other hand, having a centralized algorithm requires a huge amount of feedback information processing complexity and introduces large amounts of overhead in the calculations. The idea is to distribute the complexity in each cell, i.e. removing q index. Hence, each BS should execute the following algorithm separately.

A distributed algorithm could be derived from the above as:

$$\begin{aligned} \mathbf{b} &= \arg\max_{\mathbf{b}} \sum_{k=1}^{K} \sum_{m=1}^{M} b_{k,m,q} r_{k,m,q} \\ s.t. &\sum_{k=1}^{K} b_{k,m,q} \leq 1, \;\; m = 1, \ldots, M. \end{aligned} \tag{5}$$

Note that the second constraint is removed since it requires a centralized way of controlling all users scheduled in all cells. Thereby, one user can be scheduled in different cells at the same carrier.

This simplification distributes complexity over the network and does not require any centralized processing. Additionally, the amount of feedback can be reduced if interference is assumed to be equal to all users in all cells. That is equivalent to approximate the rate of kth user at mth carrier and qth cell as:

$$r_{k,m,q} = \log\left(1 + \frac{G_{k,m,q} p_{m,q}}{I_{m,q} + BN_0}\right). \tag{6}$$

It is easy to show that the qth cell only requires channel gains $G_{k,m,q}$ of its K users at each carrier.

4 From Spatial to Multi-cell Scheduling

In [19] the authors present a spatial scheduler for multicarrier systems in a single-cell scenario. The basis is a network flow formulation for maximization of the system sum rate. To sumarize it, the spatial diversity is solved using Multiuser Opportunistic Beamforming and choosing the user permutation, and its corresponding beam set, that achieve the best sum rate; then, the power allocation is performed from this spatial allocation. This section proposes a modification of the algorithm in [19] and distributes the spatial dimension, separating the antennas one from each others and distributing one per BS. For this reason, instead of beam-user selection, cell-user selection has to be carried out. The work in [19] considers ergodic sum rate maximization for continuous rates. The ergodic framework also allows the optimization in the time domain. In fact, if $[1, \ldots, N]$ is the time interval of the optimization, for any generic system or user metric, $R[n]$, under ergodic assumption for random processes in the system, the approximation $(1/N) \sum_n R[n] \approx \mathbb{E}\{R[n]\} = \mathbb{E}\{R\} = \mathcal{R}$ holds, where $\mathcal{R}$ does not depend on time n. Hence, optimizing $\mathcal{R}$ means optimizing $R[n]$ over time interval $[1, \ldots, N]$.

The discrete variable or index $u_{m,q} \in \mathbb{K}_0 = \{0, 1, \ldots, K\}$ indicates the user (i.e. 0 means no user) that is scheduled to use cell q on subcarrier m. Note that only one user or none can be scheduled for each carrier and each cell. The whole set of these variables is the matrix $\mathbf{U} \in \mathbb{K}_0^{M \times Q}$, whereas the whole set of powers is the matrix $\mathbf{P} \in \mathbb{R}^{+,M\times Q} \cup \{0\}$. It is implicitly assumed that if $u_{m,q} = 0$ then $p_{m,q} = 0$[1].

The aim of resource allocation is to dynamically assign radio interface resources to the different users, i.e. to determine optimal values of **U** and **P**. The problem can be formulated as

$$\begin{aligned} &\max_{\mathbf{U},\mathbf{P}} \sum_{k=1}^{K} \mathcal{R}_k(\mathbf{U},\mathbf{P}) \\ &s.t.\ \mathcal{P}_q(\mathbf{U},\mathbf{P}) \leq \bar{\mathcal{P}},\ \ \forall q \\ &\mathcal{R}_k(\mathbf{U},\mathbf{P}) \geq \phi_k \sum_{s=1}^{K} \mathcal{R}_s(\mathbf{U},\mathbf{P}),\ \ \forall k \end{aligned} \tag{7}$$

where $\mathcal{R}_k(\mathbf{U},\mathbf{P}) = \mathbb{E}\{R_k(\mathbf{U},\mathbf{P})\} = \sum_{m=1}^{M}\sum_{q=1}^{Q} \mathbb{E}\left\{\delta_k^{u_{m,q}} r_{k,m,q}\right\}$ is the rate provided to user k from (3), $\mathcal{P}_q(\mathbf{U},\mathbf{P}) = \sum_{m=1}^{M} \mathbb{E}\{p_{m,q}\}$ is the total average power spent by cell q to serve the allocated users and δ_k^u is the Kronecker's delta[2]. The first constraint refers to the total power used which must be less than a maximum amount $\bar{\mathcal{P}}$. The second constraint implies that users ought to obtain the proportional ϕ_k part of the sum rate, which determines the share of throughput finally achieved by each user. Therefore, $\boldsymbol{\phi}$ must satisfy the condition $\sum_{k=1}^{K} \phi_k = 1$.

It is important to underline that in this problem rate and power constraints are referred to as average values. In this way, the instantaneous constraints are relaxed leading to a reduction in the complexity of the resulting optimization algorithm.

4.1 Dual Optimization Framework and Adaptive Algorithms

The optimization problem is non convex and Lagrangian duality [20] is used to solve the problem. It enables each user to adapt their resources locally with the aid of limited information exchange. An interesting point of the Lagrangian is the dual decomposition into individual user and cell terms. This fact motivates decentralized algorithms as in [20] and allows to distribute the complexity over the network. However, to obtain a distributed algorithm as seen later, it is necessary to decouple user assignment from power assignment. The dual objective of problem (7) is defined as

$$\min_{\boldsymbol{\lambda}>\mathbf{0},\boldsymbol{\mu}\geq\mathbf{0}} g(\boldsymbol{\lambda},\boldsymbol{\mu}) = \min_{\boldsymbol{\lambda}>\mathbf{0},\boldsymbol{\mu}\geq\mathbf{0}} \left\{\max_{\mathbf{U},\mathbf{P}} \mathcal{L}(\mathbf{U},\mathbf{P},\boldsymbol{\lambda},\boldsymbol{\mu})\right\} = \min_{\boldsymbol{\lambda}>\mathbf{0},\boldsymbol{\mu}\geq\mathbf{0}} \mathcal{L}(\mathbf{U}^*,\mathbf{P}^*,\boldsymbol{\lambda},\boldsymbol{\mu}) \tag{8}$$

where $\mathcal{L}(\mathbf{U},\mathbf{P},\boldsymbol{\lambda},\boldsymbol{\mu})$ is the Lagrangian function of the problem (7) and $\boldsymbol{\lambda},\boldsymbol{\mu}$ are the Lagrangian multipliers.

---

[1] This also means that **P** has an implicit dependence on **U** and vice versa as shown afterwards.

[2] $\delta_k^u = 1$ if $u = k$ and 0 otherwise.

It is important to remark that while the primal problem is a non-concave maximization, the dual problem becomes a convex optimization. However, the dual problem is not differentiable and an iterative subgradient method is used to update the $K+Q$ solutions of the dual problem at each discrete time instant. Starting from initial solutions $\boldsymbol{\lambda}^0$ and $\boldsymbol{\mu}^0$, the update equations at the ith iteration derive from subgradient expressions and are:

$$\begin{aligned}
\boldsymbol{\lambda}^{i+1} &= \left[\boldsymbol{\lambda}^i - \delta_{\boldsymbol{\lambda}}\left(\bar{\mathcal{P}}_q - \mathcal{P}_q(\mathbf{U}^{*i}, \mathbf{P}^{*i})\right)\right]_\epsilon^+ \\
\boldsymbol{\mu}^{i+1} &= \left[\boldsymbol{\mu}^i - \delta_{\boldsymbol{\mu}}\left(\mathcal{R}_k(\mathbf{U}^{*i}, \mathbf{P}^{*i}) - \phi_k \sum_{s=1}^{K} \mathcal{R}_s(\mathbf{U}^{*i}, \mathbf{P}^{*i})\right)\right]^+
\end{aligned} \tag{9}$$

where $[x]_\epsilon^+ = \max(\epsilon, x),\ 0 < \epsilon \ll 1$ and $\delta_{\boldsymbol{\lambda}}$, $\delta_{\boldsymbol{\mu}}$ are positive step-size parameters. $\mathbf{U}^{*i}, \mathbf{P}^{*i}$ indicate the optimal solutions of the Lagrangian at the ith iteration, i.e. those which maximize $\mathcal{L}(\mathbf{U}, \mathbf{P}, \boldsymbol{\lambda}^i, \boldsymbol{\mu}^i)$.

4.2 Solutions for the Allocation Problem

The optimal power and user solutions are difficult in that case due to the cross dependence of user and power allocation. Therefore, the dual objective can be rewritten as follows:

$$g(\boldsymbol{\lambda}, \boldsymbol{\mu}) = \max_{\mathbf{U},\mathbf{P}} \mathcal{L}\left(\mathbf{U}, \mathbf{P}, \boldsymbol{\lambda}, \boldsymbol{\mu}\right) = \sum_{q=1}^{Q} \lambda_q \bar{\mathcal{P}} + M\mathbb{E}\left\{\max_{\mathbf{u}_m}\left[\max_{\mathbf{p}_m \geq \mathbf{0}} \mathcal{M}(\mathbf{u}_m, \mathbf{p}_m)\right]\right\} \tag{10}$$

with

$$\mathcal{M}(\mathbf{u}_m, \mathbf{p}_m) = \sum_{q=1, u_{m,q} \neq 0}^{Q} \left[(\mu_{u_{m,q}} - \boldsymbol{\mu}^T \boldsymbol{\phi}) \log_2(1 + r_{u_{m,q},m,q}(\mathbf{p}_m)) - \lambda_q p_{m,q}\right]. \tag{11}$$

The optimal solution, given $\boldsymbol{\lambda}, \boldsymbol{\mu}$, becomes, for each frequency m,

$$\mathbf{u}_m^* = \arg\max_{\mathbf{u}_m} \mathcal{M}^*(\mathbf{u}_m) \tag{12}$$

with

$$\mathcal{M}^*(\mathbf{u}_m) = \max_{\mathbf{p}_m \geq \mathbf{0}} \mathcal{M}(\mathbf{u}_m, \mathbf{p}_m). \tag{13}$$

This shows that user selection (12) and power allocation (13) are decoupled from the dual optimization and both them can be computed separately. In fact, user selection is computed before the power solution is found.

Concerning spatial allocation, the main issue is to reduce the search space. This issue can be faced by using suboptimal greedy selection procedures. The simplest among them is the opportunistic selection. Thereby, each user selects the best cell by assuming that all base stations are transmitting with a preassigned power and feeds back the selected cell with its SINR, while each cell allocates its resources to the best user selected among those competing for that cell. This can be done helped by spatial beamforming at each base station. Next sub-section comments further on that.

4.3 Discussion on Centralized and Distributed Solutions

The optimal solution requires a centralized controller that runs all or parts of the algorithms. Even though the power allocation algorithm based on the update of $\boldsymbol{\lambda}^i$ can be distributed on each base station, user allocation algorithm requires a centralized solution, i.e. a controller which knows all channel gains determines, for all subcarriers, the vector $\mathbf{u}_m$ and send it to base stations through signaling.

A decentralized implementation can be set up by using the opportunistic suboptimal solution of power allocation. In this case user allocation algorithm has two steps (for each subcarrier):

- Each user selects the best cell by assuming that all base stations are transmitting with a preassigned power and feeds back the selected cell with its SINR.
- Each base station allocates its resources to the best user selected among those competing for that cell. When user allocation is decentralized, two points need to be remarked.

The first one is related to the update of $\boldsymbol{\mu}^i$ .This can be performed at the base stations, if users are served by only one base station, or it can be performed by the users after that the information on the resource allocation is sent to them. The second one is related to the evaluation of the user rates. This can be done based on the SINR evaluated by the user, which does not take into account the powers actually allocated to interfering users, because they are not known. Therefore, the allocated rate is not the actual rate supported by the transmission leading to possible outages. This can be avoided only by evaluating the SINR by using the worst-case values of interfering power in the vector $\mathbf{V}_m$, which can be further constrained to be less than a maximum value P_{max} on each resource unit.

To counteract the losses that opportunistic schemes present when the number of users is moderate or low[3], while still preserving a decentralized implementation, the "power planning" concept (as [21] for time-division multiple access systems) can be introduced to preassign suitable power values to vector $\mathbf{V}_m$ with the additional constraint $p_{m,q} \leq v_{m,q}$.

5 Conclusions

Multi-cell scenarios are present in a very large number of standards and systems. The trends of technology and the increased requirements in bandwidth usage efficiency dictate the tight re-use of the frequency bands in neighboring cells. To

---

[3] When the number of users is not very large, sum rate is maximized by allocating a number of users on each subcarrier and slot usually smaller than Q.

do that, effective interference management schemes are required to regulate optimally the transmitted power in each subcarrier in all cells. In this context, power planning was presented as a suitable tool to extract effective network parameters and requirements. Additionally, layered and distributed dynamic resource allocation algorithms were introduced in those scenarios that have predefined rate requirements and power may be adjusted to guarantee the provided QoS. Finally, cross-laying for multi-cell user scheduling is focused by Lagrangian duality to solve the same problem and ensure the QoS constraints.

References

1. Avdikos, G., et al.: New Scheduling Techniques and Design Paradigms for Multi-Carrier and Space Division Systems, Self-Organising and Distributed Networks. NEWCOM++ DR.8.2 (2009)
2. Gesbert, D., Kountouris, M., Heath, R.W., Chae, C.-B., Salzer, T.: Shifting the MIMO Paradigm. IEEE Signal Processing Magazine 24(5), 36–46 (2007)
3. Coso, A.D., Savazzi, S., Spagnolini, U., Ibars, C.: Virtual MIMO Channels in Cooperative Multi-hop Wireless Sensor Networks. In: 40th Annual Conference on Information Sciences and Systems, pp. 75–80 (2006)
4. Simeone, O., Somekh, O., Poor, H.V., Shama, S.: Distributed MIMO systems with oblivious antennas. In: IEEE International Symposium on Information Theory, ISIT 2008 (2008)
5. Gesbert, D., Kiani, S.G., Gjendemsj, A., Oien, G.E.: Adaptation, Coordination, and Distributed Resource In: Allocation in Interference-Limited Wireless Networks. Proceedings of the IEEE (2007)
6. Kiani, S.G., Gesbert, D.: Optimal and Distributed Scheduling for Multicell Capacity Maximization. IEEE Transactions on Wireless Communications 7(1), 288–297 (2008)
7. Goodman, D., Mandayam, N.: Power control for wireless data. IEEE Pers. Commun. Mag. 7, 48–54 (2000)
8. Yates, R.D.: A framework for uplink power control in cellular radio systems. IEEE J. Sel. Areas Commun. 13(7), 1341–1347 (1995)
9. Chawla, K., Qiu, X.: Quasi-static resource allocation with interference avoidance for fixed wireless systems. IEEE J. Sel. Areas Commun. 17(3), 493–504 (1999)
10. Gesbert, D., Kountouris, M.: Joint Power Control and User Scheduling in Multicell Wireless Networks: Capacity Scaling Laws. IEEE Trans. Inf. Theory (2007)
11. Jing, S., et al.: Multicell Downlink Capacity with Coordinated Processing. In: Eurasip JWCN (2008)
12. Simeone, O., Somekh, O.: Downlink Multicell Processing with Limited-backhaul Capapcity. In: Eurasip JSAC (2009)
13. Kobayashi, M., et al.: Outage Efficient Strategies in Network MIMO with Partial CSIT. In: IEEE ISIT 2009 (2009)
14. Dahrouj, H., Yu, W.: Coordinated beamforming for the Multi-Cell Multi-Antenna Wireless System. In: CISS, New Jersey (2008)
15. Luo, Z.Q., Zhang, S.: Dynamic spectrum management: complexity and duality. IEEE J. Sel. Topics Signal Process., Special Issue on Signal Processing and Networking for Dynamic Sprectrum Acess 2(1), 57–73 (2008)
16. Liu, Y.-F., Dai, Y.-H., Luo, Z.-Q.: On the Complexity of Optimal Coordinated Downlink Beamforming. In: ICASSP (2010)

17. Dainelli, G., Moretti, M., Zalonis, A., Dimitriou, N.: Distributed Radio Resource Allocation Schemes in OFDMA Cellular Networks. In: ICT Future Network & Mobile Summit, Florence, Italy, June 16-18 (2010)
18. Moretti, M., Todini, A.: A Resource Allocator for the Uplink of Multi-Cell OFDMA Systems. IEEE Transactions on Wireless Communications 6(8), 2807–2812 (2007)
19. Perez-Neira, A., Henarejos, P., Tralli, V., Lagunas, M.A.: A low complexity space-frequency multiuser resource allocation algorithm. In: International ITG Workshop on Smart Antennas (WSA 2009), Berlin (2009)
20. Chiang, M., Zhang, S., Hande, P.: Distributed rate allocation for inelastic flows: optimization frameworks, optimality conditions, and optimal algorithms. IEEE J. Sel. Areas Commun. 23(3), 2679–2690 (2005)
21. Tralli, V., Veronesi, R., Zorzi, M.: Power-shaped advanced resource assignment (PSARA) for fixed broadband wireless access systems. IEEE Trans. on Wireless Comm. 3(6), 2207–2220 (2004)

Multi-hop Relay in Next Generation Wireless Broadband Access Networks: An Overview

Nikos Athanasopoulos, Panagiotis Tsiakas, Konstantinos Voudouris,
Iraklis Georgas, and George Agapiou

Department of Electronics, Technological Educational Institution of Athens,
Agiou Spiridonos, 12210 Athens, Greece
{nathan,pantsiak,kvoud,ira}@ee.teiath.gr
Wireless and Satellite Communications Research Lab.,
Hellenic Organization of Telecommunications
99 Kifisias Av., 15124 Athens, Greece
gagapiou@oteresearch.gr

Abstract. Relay technologies have the potential to offer extended cell coverage and improved capacity over the Next Generation Wireless Broadband Radio Access Networks. Standards development organizations are considering how to incorporate relay technologies into new standards. This article provides an overview of the relay-based technology concepts for two of the most promising next generation wireless broadband networks: WiMAX and LTE, focusing on some of the most pertinent aspects. In particular, the various potential relaying scenarios are described, while the integration and adaptation of the Multi-hop Relay in the framework of WiMAX and LTE networks is analyzed. Some consideration of the issues in designing such systems is also given, which highlights when different features within the standard are most appropriate. As these systems are very new, many open issues remain to be resolved.

Keywords: Next Generation Wireless Broadband Access Networks, WiMAX, LTE, Multi-hop Relay technologies, Relay Station.

1 Introduction

The rapidly growing demand for affordable bandwidth in fixed and mobile services is driving the telecommunications and advanced technologies industries to deliver high performing, cost effective wireless broadband platforms that can be deployed in the varied spectral allocations worldwide [1]. These platforms, addressing the bandwidth demands, share key technology enablers including Orthogonal Frequency Division Multiplexing (OFDM) air interface, advanced antenna techniques including Multiple-Input-Multiple-Output (MIMO) and beamforming, flat all IP architectures, etc [2].

The major next generation wireless broadband access platform candidates are Worldwide Interoperability for Microwave Access (WiMAX) and Long Term Evolution (LTE). These two platforms meet the needs for fixed, nomadic and mobile communications, including voice, data, video, gaming and personal broadband, in enterprise, residential, underserved, campus, special events, wholesale and safety & security applications [2]. In order for WiMAX and LTE to deliver ubiquitous broadband content,

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 543–554, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

the network is required to provide excellent coverage both outdoor and indoor and significantly higher bandwidth per subscriber. The wireless Multi-hop Relay Station technologies currently receive much interest as they intend to fulfill these challenges [3]. The major benefit of these techniques leads to the fact that a Relay Station does not require any dedicated backhaul equipment as it receives its capacity from centralized base stations via the same resources used for the access service.

The rest of the paper is organized as follows: A brief overview on WiMAX and LTE standards is given first. Multi-hop relay networks basic concepts and how they are adopted in WiMAX and LTE platforms is then presented. Finally, the most common multi-hop relay scenarios are described.

2 WiMAX and LTE Standards Overview

2.1 WiMAX (802.16e and Beyond)

WiMAX technology evolution initially started with the IEEE802.16d [4]. Next step was NWG 802.16e Release 1.0 [5], [6], defined by Network Working Group (NWG) of WiMAX Forum. Release 1.5, which provides backwards compatible with Release 1.0 is expected in 2010. Finally, WiMAX Forum expects to specify 802.16m like the future WiMAX technology in order to get the 4G challenges. 802.16m provides higher data rates, reduced latency and efficient security mechanism. The availability of this release is expected in 2012. Mobile WiMAX air interface characteristics are summarized in Table 1.

Table 1. Mobile WiMAX Air Interface characteristics

Characteristic	Description
Channel Bandwidth	5, 7, 8.75 and 10 MHz
DL multiple access	OFDMA
UL multiple access	OFDMA
Duplexing	Time Division Duplexing (TDD)
Subcarrier mapping	Localized and distributed
Subcarrier hopping	Yes
Data modulation	QPSK, 16QAM and 64QAM
Subcarrier spacing	10.94 KHz
FFT size (5 MHz)	512
Channel coding	Convolutional coding and convolutional turbo coding
MIMO	Beamforming, Space-time coding and spatial multiplexing

In terms of network features, WiMAX Forum NWG [6], [7] defines a reference architecture for the WiMAX network interconnection with other networks, which is independent of the radio interfaces. A set of reference points has been specified, including interfaces, protocols and procedures. Fig. 1 represents a logical-functional architecture of the WiMAX network. A set of functional entities and reference points are identified. The entities are described as follows: *SS/MS (Subscriber Station/Mobile Station)* providing network connectivity to the user, *ASN (Access Service Network)* providing radio connectivity to the users and *CSN (Connectivity Service Network)* providing IP connectivity.

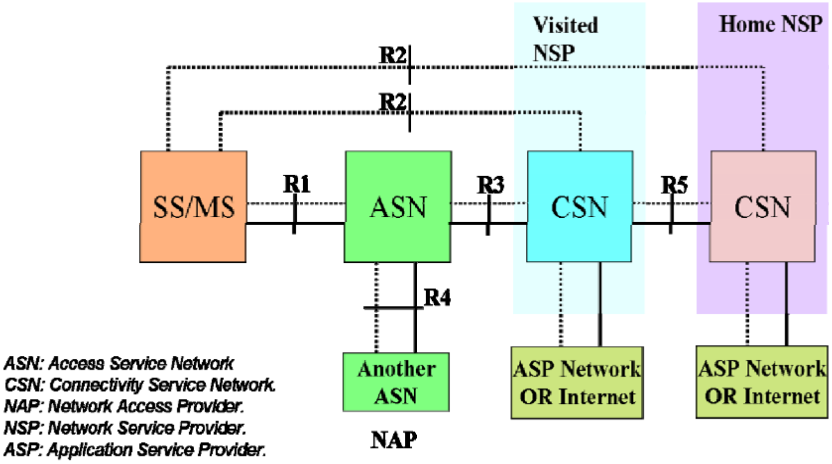

Visited NSP
Home NSP
R2
R2
SS/MS
R1
ASN
R3
CSN
R5
CSN
R4
Another ASN
ASP Network OR Internet
ASP Network OR Internet
NAP
ASN: Access Service Network
CSN: Connectivity Service Network
NAP: Network Access Provider.
NSP: Network Service Provider.
ASP: Application Service Provider.

Fig. 1. Reference Architecture of the WiMAX Network

2.2 LTE and LTE-Advanced

LTE [8] is the project within 3GPP designed to improve UMTS standard to cope with future technology evolutions. LTE defines a high-speed radio access method for mobile communication systems and offers a path for operators deploying 3GPP and non-3GPP technologies to higher speeds and lower latency [9]. 3GPP standard evolution started with release 99 that specified UMTS/WCDMA technology. Next step was HSDPA and HSUPA technologies specified in Release 5 and 6 respectively. Release 7 specified HSPA+, the link between HSPA and LTE. Today, LTE specifications are encapsulated in Release 8, which was finalized and approved in January 2008 and it is target deployment in 2010. 3GPP has also started to work in the next evolutionary broadband systems, called LTE-Advanced. Table 2 summarizes LTE air interface characteristics.

Table 2. LTE Air Interface characteristics

Characteristic	Description
Channel Bandwidth	1.4, 3, 5, 10, 15 and 20 MHz
DL multiple access	OFDMA
UL multiple access	SC-FDMA
Duplexing	FDD and TDD
Subcarrier mapping	Localized
Subcarrier hopping	Yes
Data modulation	QPSK, 16QAM and 64QAM
Subcarrier spacing	15 KHz
FFT size (5 MHz)	512
Channel coding	Convolutional coding and turbo coding
MIMO	Multi-layer precoded spatial multiplexing space-time/ frequency block coding, switched transmit and cyclic delay diversity

In terms of network features, LTE supports flat all-IP network architecture allowing interworking with legacy 3G networks and high mobility between heterogeneous access networks. In addition, LTE is expected to substantially improve end-user throughput, sector capacity and reduce user plane latency [10]. To achieve these challenges, the global LTE network architecture is composed of: *Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)* been composed of eNodeB (eNB) elements and *Evolved Packet Core (EPC) architecture* supporting E-UTRAN through the reduction in the number of network elements.

From a high level point of view, LTE architecture consists of the following functional elements: *eNodeB (eNB)* which is the base station in LTE access network and is in charge of all radio interface-related functions, *Mobility Management Entity (MME:* which is in charge of managing mobility, *Serving Gateway (S-GW)* which routes and forwards user data packets and *Packet Data Network Gateway (PDN-GW)* which provides connectivity to the UE to external packet data networks.

Fig. 2 illustrates the high level architecture for LTE and the interconnection between all the functional elements [10].

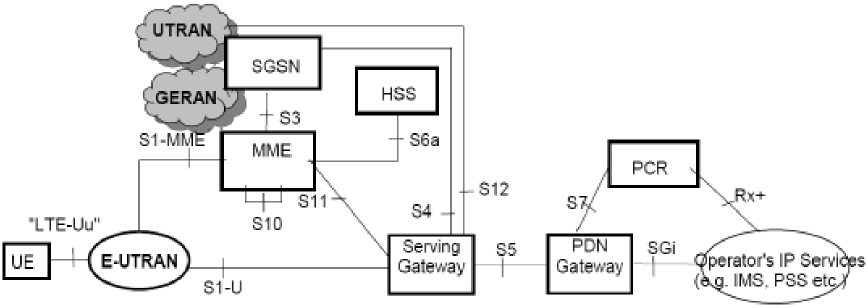


Fig. 2. LTE Network Architecture

3 Multi-hop Relay Networks

The current backhaul network architectures are based primarily on leased lines. This is inadequate for offering future broadband services. Moreover, coverage improvement and capacity enhancement are always the essential requirements for wireless broadband networks in order to deliver cost-effective wireless services. Due to the higher demand for high quality multimedia applications, capacity enhancement is a must for the next generation cellular networks. Furthermore, as the data rate demand of mobile applications increases, the effective coverage range given a fixed transmit power becomes less.

Initially, this problem has been addressed by deploying stations in a denser manner. However, the high manufacturing, deployment and maintenance cost render this approach less desirable. Multi-hop relay technology was created to deal with these issues. It is a cost-effective deployment because relay stations do not need wired backbones. The technique of augmenting cellular networks with multi-hop relay networks has been applied to different types of wireless network with the main objectives of enhancing cellular coverage, increasing system throughput, helping overcome obstacles, balancing load within wireless access networks, providing flexible wireless network access and finally helping decrease the cost since they are much cheaper than base stations.

Nowadays, multi-hop relay networks have become promising wireless networking architecture for future wireless access system and relay technology is being standardized by different forums and organizations. Relays are being standardized in WiMAX technology through the IEEE 802.16j working group, which enhances multi-hop relay defined in IEEE802.16e. 3GPP organization is also working on relay technology (3GPP named stations "repeater"), based on communication relaying protocol proposed for UMTS TDD mode to be applied in LTE technology.

3.1 Multi-hop Relay in WiMAX Networks

There are various choices available for WiMAX networks operators to improve indoor or outdoor coverage or to increase network capacity. These choices include different types of base stations: macrocells, microcells, or picocells in an outdoor environment, picocells in public indoor locations or within enterprise buildings, and femtocells for residential. The primary difference between them is the size of coverage. Macrocells have the longest range, but are also the most expensive to purchase, deploy and maintain. Micro, pico and femto base stations are used to fill in coverage gaps and establish coverage in buildings where the macrocell signals can hardly penetrate. A significant side-effect of placing a large number of base stations in a region is that each needs a dedicated broadband backhaul connection. Micro, pico, and femto cells can use wireless links for their backhaul. In particular, they can support in-band backhaul to enable operators to use their spectrum holdings to carry backhaul traffic to the nearest macro base station.

IEEE 802.16j working group is responsible for generating a standard for WiMAX Mobile Multi-hop Relay (MMR) network. A set of technical issues are specified in order to enhance previous standards (IEEE 802.16e) with relay support.

Multi-hop Relay Station (RS) provides additional coverage or performance advantage in an access network. In RS networks, the Multi-hop Relay BS (MR-BS) is connected to several Relay Stations (RSs), in a multi-hop topology, in order to enhance the network coverage and capacity density. Traffic and signaling between the Mobile Subscribers (SS) and MR-BS are relayed by the RS thereby extending the coverage

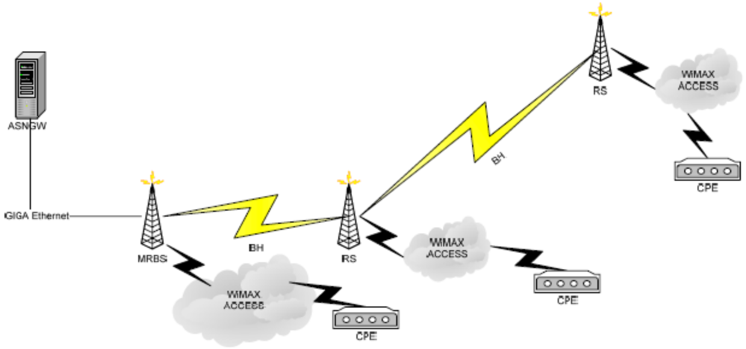


Fig. 3. A two-hop Relay Station deployment example

and performance of the system in areas where RSs are deployed. Each RS is under the supervision of an MR-BS. In a system with more than two hops, traffic and signaling between an access RS and MR-BS may also be relayed through intermediate RSs. The RS is fixed in location. The MS may also communicate directly with the MR-BS. Fig. 3 illustrates the MR-BS and two-hop RS deployment. For each of the RS there is an ACCESS link that covers the current cell and a BACKHAUL link to the next cell.

The interconnection between these nodes includes the following link classification:

Table 3. Relay 802.16j links

Links	Description
MR-BS to MS	The MR-BS can associate with multiple MSs
RS to MS	The RS can associate with multiple MSs
MR-BS to RS	The MR-BS can associate with multiple RSs

The main technical issues being discussed in the IEEE 802.16j work group are new frame structure to support Relay Stations, centralized vs. distributed control, centralized vs. distributed scheduling, radio resource management, power control, call admission and traffic shaping policies, QoS based on network wide load balancing and congestion control, security and management.

Focused on NWG reference architecture, Fig. 4 identifies the reference points and the functional entities in which relay technology should be included. A new ASN entity, called ASN-Relay, is focused on relay concepts. This entity will establish all relay network functionality defining a new reference points called R1', which consists of the protocols and procedures to establish the communication links defined above. Moreover, it will be compatible with R1 and R6 reference points, because RSs and MRBS must be compliant with IEEE802.16e standards.

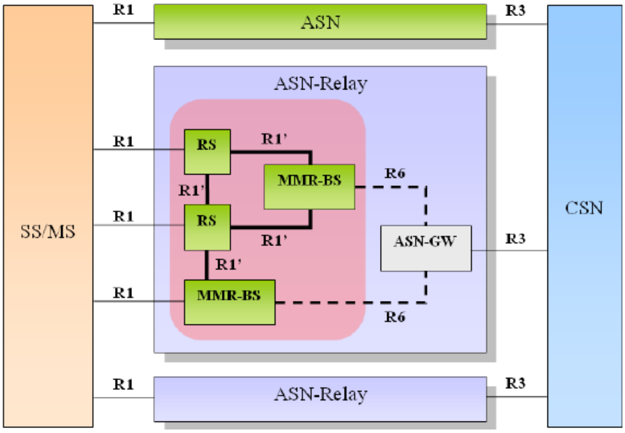


Fig. 4. Relay Technology Proposal in NGW Reference Architecture

3.2 Multi-hop Relay in LTE Networks

LTE, which promises real data rates up to 100 Mbps and by using MIMO antennas it can reach few hundred of Mbps, is almost complete. Consequently, the usage of relay stations in LTE networks appears to be inevitable. LTE Advanced, which will include relay stations, is in process of being standardized by the 3GPP for Release 10. However, there are many issues regarding the introduction of relay stations in LTE networks that must be taken into consideration. Among them the most important are the frame structure to be used due to the existence of relay stations, the transmission power control algorithm, a method to overcome interferences among random access signals and backward compatibility. There is a continuously increasing demand for high spectral efficiency for a certain geographical area that will be satisfied by the use of multi-hop relay stations in an LTE network. But there is also a demand of smaller cell sizes in order to achieve the previous. If this should be implemented only with conventional base stations (eNBs) it would result in high cost for eNB deployment and operation. Therefore, small eNB cells can be replaced by relay 'cells' at reduced backhaul cost.

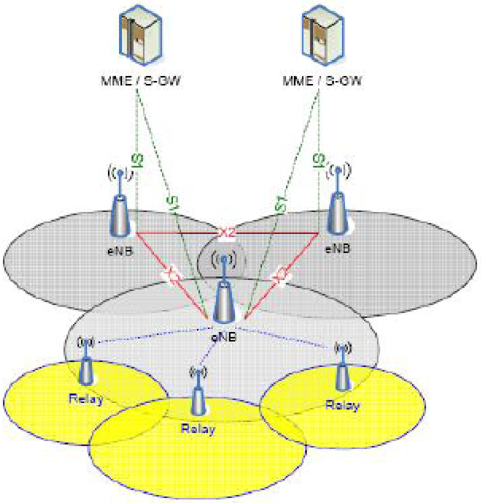


Fig. 5. Relay Technology Proposal in NGW Reference Architecture

3GPP has considered two deployment scenarios of relay nodes. The first scenario considers that the coverage of the cell is provided by an LTE eNodeB. The serving eNodeB supports direct connections to and from LTE-Advanced UE and legacy LTE UEs while a relay station may be deployed in the cell for providing additional coverage at cell-edge or coverage holes to all UEs that are located in these areas. UEs communicate with the serving eNodeB in uplink and downlink direction through the intermediate relay station(s). The other scenario includes a legacy LTE eNodeB serving the area. The requirements are the same as in the first scenario with the only difference that legacy NodeB is obliged to be capable of connecting to relay station.

Relay stations can be transparent and non-transparent. Transparent relays mean that UE is not aware of whether it communicates or not with the network via relay. Transparent relay has certain advantages in the sense that it will introduce no impact to the UE so it could be used to improve the coverage and cell-edge throughput for LTE Advanced and Release 8 system. On the other hand, if a relay station is going to be deployed to support LTE advanced UEs as a non-transparent relay, it could be used to function as transparent relay for certain Release 8 UEs. In this case, no additional deployment cost will be needed.

4 Multi-hop Relay Scenarios

A RS can be adapted at several mobility levels, i.e. fixed, nomadic, mobile, and can be used in the Next Generation Networks for improving the communication quality by several aspects, depending on the user needs and the environment conditions and constraints. In this section, the most common relay scenarios are described.

4.1 Hole Filler

A RS can be used inside the service area of the cell in order to improve link quality to those specific areas that do not have sufficient link quality due to excessive link attenuation from the BS. This attenuation can be caused among other factors due to shadowing of buildings or due to a given hilly topography. Such a scenario is shown in Fig. 6.

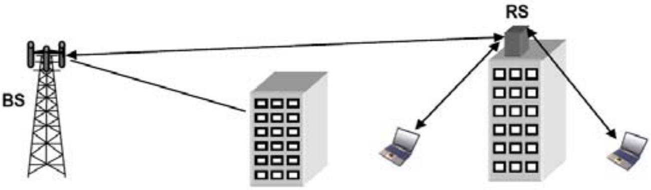


Fig. 6. Hole Filler Relay Station Scenario

4.2 Cell Extension

In this case, a RS is used to increase the coverage area of a cell. A RS can extend the coverage area in a certain location at the edge of the cell as shown in Fig. 7a or cover an area separated from the coverage area of the cell as shown in Fig. 7b. This latter configuration is sometimes called "remote sector". Cell extension can be used in a more strategic manner where multiple RSs are deployed around the perimeter of a cell to achieve higher coverage area with a single BS, as shown in Fig. 7c. This concept may be used as a part of the network design strategy in order to provide coverage with as few as possible base stations.

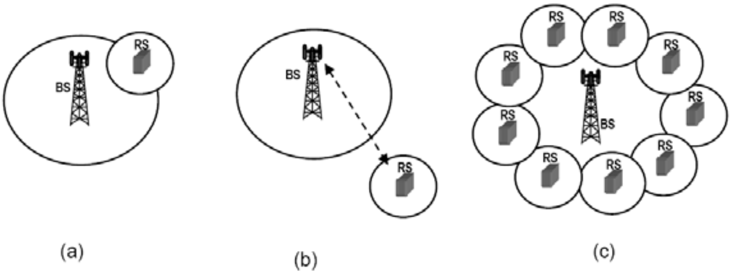


Fig. 7. Cell Extension Relay Station Scenario

4.3 Capacity and Throughput

In most scenarios, the use of an RS can increase the per-MS throughput, system capacity and QoS. A single link between the BS and RS with high Signal to Interference plus Noise Ratio (SINR) (and as a result with high order modulation and coding scheme) can be replaced with multiple RS to BS links with low SINR. The result is an increase in spectral efficiency which produces a capacity increase. This additional capacity can be used for providing higher throughput to individual MSs or to support more MSs within the coverage area of the RS. In addition, the link reliability is enhanced due to improved SINR.

Fig. 8 depicts a scenario where four RSs are deployed in the service area of a sector. The capacity of the original coverage area may increase by a factor of four due to the fact that each RS provides its own capacity to the area and MSs which had low quality link to the BS may have better link quality to the serving RS. This increase in link quality is translated by the inherent link adaptation process to higher throughput and therefore to a higher capacity.

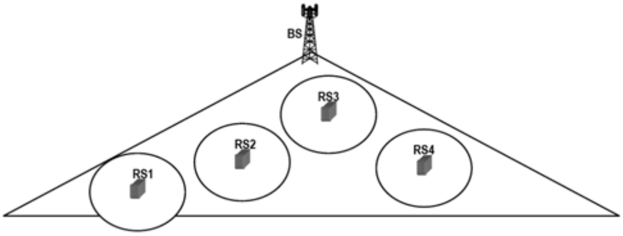


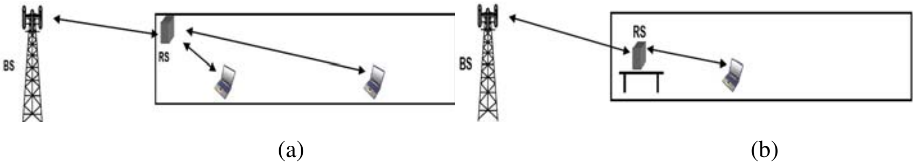
Fig. 8. Capacity and Throughput Improvement Relay Station Scenario

4.4 Indoor Usage Scenarios

The majority of cellular traffic is generated from buildings. Providing service to indoor MSs by the same BS that provides service to outdoor MSs has several major disadvantages. First, due to the building walls introduced attenuation, BS-MS link might be marginal or of a low quality thus limiting the data rate and consuming excessive time-frequency resource from the BS. MSs which reside in high floors of a building, pose another issue. They are exposed to multiple BSs arriving signals and as a result, two problems may occur: First, signals may interfere with each other, hence degrading the SINR of the MS. Second, MS may enter into an undesired hand off process and as a result, excessive handover processes might occur. This may result in power consumption of the radio, backhaul and computational resources.

Relaying technologies in indoor environments can be proved challenging in order to improve the communication. The major methods used for providing dedicated coverage for indoor MSs are described below.

Fixed and Nomadic RS with direct connection to the BS. A fixed RS is mounted in a way that its antenna maintains good link quality concurrently with the BS and with the MSs which reside in the building. Alternatively, the RS may be lightweight, nomadic, similar to a WiFi router.



(a) (b)

Fig. 9. A Relay Station with direct connection to the Base Station in an indoor scenario. In (a) the Relay Station is Fixed, while in (b) the Relay Station is Nomadic.

Multi-hop RS. When large area floors need to be covered, a single RS may not be sufficient. In such cases, multiple RSs can be distributed over the floor connected to each other using the multi-hop capability. The internal RSs can be chained to a RS mounted at the edge of the floor with a good link to the BS as depicted in Fig. 10.

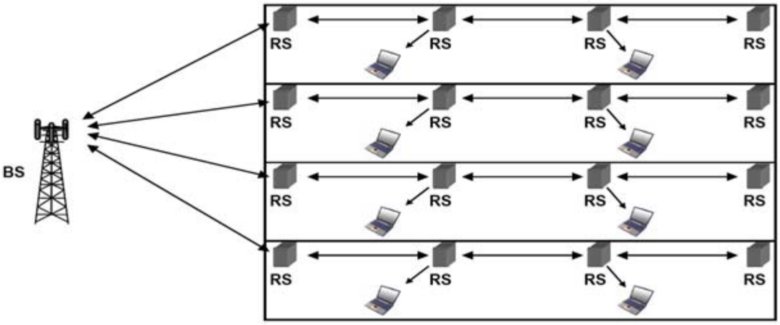


Fig. 10. A Multi-hop Relay Station indoor scenario

Coverage with dedicated external RSs. In some cases it may possible to provide in-building coverage with external RSs "illuminating" the building from outside as depicted in Fig. 11. The advantage of this model is the elimination of the excruciating need for installing equipment and cabling inside the building.

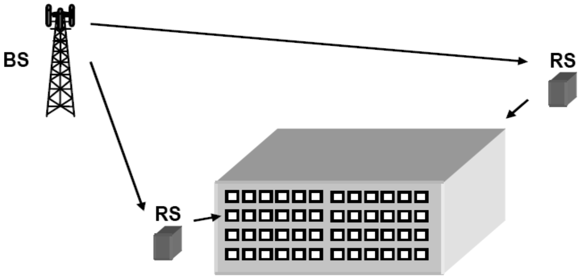


Fig. 11. Two external Relay Stations illuminating a building

4.5 Road and Tunnel

The common requirement for roads and tunnels is the need to provide coverage along a linear path. Since high mobility MSs are served, it is recommended to allow the move without handover between the coverage area of each RS. Fig. 12 depicts a scenario where a BS feeds in parallel three transparent RSs. This configuration allows continues high SINR connection along the road without handover.

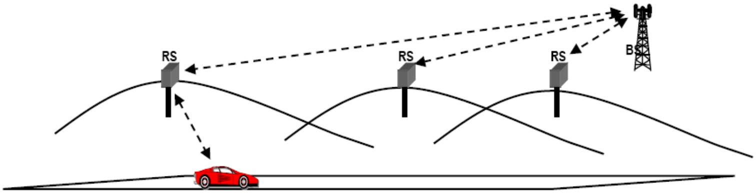


Fig. 12. A Base Station feeds three Relay Stations in parallel

Fig. 13 shows a tunnel covered by RSs. The RSs inside the tunnel have no connection with the external BSs and therefore multi-hop RSs must be used. In order to minimize the number of hops, the internal RSs can be split to two groups each fed from a BS at each side of the tunnel.

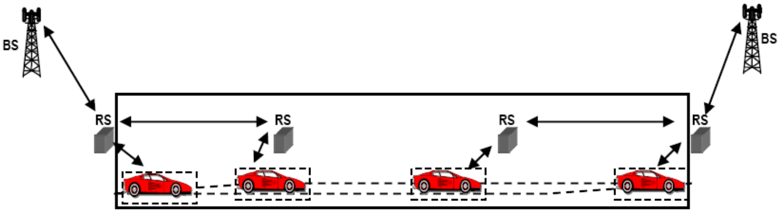


Fig. 13. A tunnel coverage through a multi-hop Relay Station configuration

4.6 Temporary Relay Stations

RSs may be deployed temporarily to provide coverage or additional capacity. An example would be in events where a heavy load on the network is expected only in certain predefined time interval such as sporting events, concerts or other events where a large crowd is expected to gather. In the case of adding capacity to an area where an event takes place, usually reasonable coverage from the macro BS already exist. In another usage model a relay can be used for providing coverage in areas where network coverage is needed temporarily for an incidental reason. An example would be an emergency incident or a disaster recovery effort where fixed infrastructure network has been destroyed overloaded or never existed before. Service to that cases can be provided by a deployment of temporary RS usually suitably installed on a vehicle.

Acknowledgments. The present work has been performed in the scope of the REWIND ("REIay based WIreless Network and StandarD") European Research Project and has been supported by the Commission of the European Communities–Information Society and Media Directorate General (FP7, Collaborative Project, ICT-The Network of the Future, Grant Agreement No. 216751).

References

1. ITU-R Rep. M.2134: Requirements Related to Technical Performance for IMT-Advanced Radio Interface(s), (2008)
2. Motorola White Paper: Driving 4G: WiMAX & LTE (2008)
3. Genc, V., Murphy, S., Yu, Y., Murphy, J.: IEEE 802.16j Relay-based Wireless Access Networks: An Overview. IEEE Wireless Communications Magazine Special Issue on Recent Advances and Evolution of WLAN and WMAN Standards (2008)
4. IEEE Std. for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems (2004)
5. IEEE Std. for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1 (2006)
6. WiMAX Forum: WiMAX End-to-End Network Systems Architecture. Stage 2: Architecture Tenets, Reference Model and Reference Points. Release 1, v1.2.2., Network Working Group (2008)
7. WiMAX Forum: WiMAX End-to-End Network Systems Architecture. Stage 3: Detailed Protocols and Procedures. Release 1, v1.2.2., Network Working Group (2008)
8. Long Term Evolution (LTE)/ System Architecture Evolution (SAE), `http://www.3gpp.org/Highlights/LTE/lte.htm`
9. UMTS Forum White Paper: Towards Global Mobile Broadband. Standardizing the future of mobile communications with LTE (Long Term Evolution) (2002)
10. Myung, H.G.: Technical Overview of 3GPP LTE (2008)

An Experimental MIH Platform for Testing Video Streaming Services across Heterogeneous Radio Access Technology Networks

Lampros Dounis[1], Michail Tsagaropoulos[1], Ilias Politis[1], and Tasos Dagiuklas[2]

[1] Department of Electrical and Computer Engineering,
University of Patras, Rio 26500, Greece
[2] Department of Telecommunication Systems and Networks
TEI of Mesolonghi, Nafpaktos 30300, Greece
dounis@gmail.com, mtsagaro@ece.upatras.gr,
ipolitis@ece.upatras.gr, ntan@teimes.gr

Abstract. This paper presents an experimental wireless platform allowing the seamless handoff of mobile terminals with on-going video sessions across heterogeneous radio access technology networks. The handover decision is taken by considering parameters from the physical and network layers from both the mobile terminal and radio access networks using Media Independent Handover (MIH) concept. It is demonstrated that when the network is congested, triggering handover from MIH improves and maintains the perceived video quality of service.

Keywords: Vertical Handover, Seamless Mobility, MIH, Video over Wireless.

1 Introduction

The last few years, the rapid evolution of wireless technologies have further increased the heterogeneity of the wireless radio access networks (HSDPA, WiMAX, 802.11g, LTE) 1. Along with the wireless evolution, there are available advanced mobile terminals that support more than one type of wireless connectivity (e.g. WLAN, 3G). Next Generation Networking (NGN) aims to provide a single All-IP network architecture that will converge heterogeneous access networks and services and leave back the "Single network per service" design of the past. This convergence will give the ability to the mobile terminals to be Always Best Connected (ABC) 2. This philosophy is also referred as connected anywhere, anytime and anyhow and it is based on the idea that a mobile terminal can choose the best available network that will cover its QoS requirements (throughput, delay, packet loss) and user's preferences (cost, security, QoE) 3.

Until today, the handover decision functionality was triggered by the physical and link layers (i.e. SNR drops below a threshold) and totally ignoring both network and application layer metrics. The main challenge for a transparent seamless mobility is to consider both network and application layer requirements 3. As an effect, having full knowledge of the current and candidate neighbor networks the handover decision can

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 555–566, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

be optimized. That is the approach that has been adopted by Media Independent handover framework in 2003, IEEE with the 802.21 Media Independent Handover (MIH) came to standardize the way of which the network and the terminals exchange information, events and handover commands for an optimal seamless handover between heterogeneous networks 4.

With the increase of the bandwidth in the wireless networks and the encoding bit rate due to advanced encoding technologies (H.264), video services have evolved (i.e. Mobile TV, VoD, Live Streaming) to cover the increasing users' desires and are now one of the most used services in wired and wireless networks. However, video services create one of the most demanding traffic for wireless networks. Video traffic demands high throughput, low delay and packet loss. While, packet loss at wired networks reveal congestion this is not a fact for the wireless networks where packet loss can be due to interference from external sources or loss of signal. MIH is a framework that will give the ability to maintain the video QoS by selecting the best candidate network

The aim of this paper is to examine the impact of handovers in the QoS of ongoing video services under the MIH framework. Having no other option but moving to another available network, MIH will provide the essential information to make the optimal choice. This Paper is organized as follows: Section 2 describes the MIH Framework, Section 3 presents the design and implementation of the experimental MIH platform, Section 4 analyses test cases and performance evaluation results and Section 5 concludes the paper.

2 Seamless Handover across Heterogeneous RATs, IEEE-802.21 Media Independent Handover (MIH) Framework

IEEE created the 802.21 standard in order to challenge one of the main issues in wireless mobility, seamless handovers across inter-technology RATs. Mobility protocols such as Mobile IP are suffering from sensible latency and they have not knowledge about the application layer parameters and candidate network conditions 4. IEEE 802.21 proposes the MIH Framework where mobile nodes and the network exchange information and commands for an optimal handover. Entities that are responsible for the handover procedure receive information and events from the MIH services and execute the handover with the available standardized commands. For hiding the heterogeneity of the MAC and PHY layers, MIH inserts an intermediate layer between layer 3 (and above) and the divert Layer 2 technology specifics. This new abstract layer is referred as Media Independent Function (MIHF) and provides a media-independent interface to the MIH users (i.e. mobility protocols, applications, handover policies) for controlling and getting information from the lower layers (i.e. WLAN, 3GGP). The communication between these three entities is grouped into three different Service Access Points (SAPs): MIH_SAP, MIH_LINK_SAP and MIH_NET_SAP 5.

- MIH_SAP enables the communication between the MIH users and the MIHF.
- MIH_LINK_SAP allows the communication between the MIHF and the link layers. MIHF takes care of handling Link layer events and passing this information to the upper layers as well as translating upper layers commands to Link

layer commands. Actually it is mapping of MIH_LINK_SAP primitives to technology-dependent Link layer SAPs.
- MIH_NET_SAP makes feasible the communication between the MIHF entities

The communication between the MIHF entities of the network makes handoff a cooperative procedure between the client and the network. Thus, handoff may be originated either by the network, by the client or by the client with assistance from the network.

The MIH framework (Fig. 1) describes three different types of communication that act as services 6: Event Service, Command Service and Information Service.

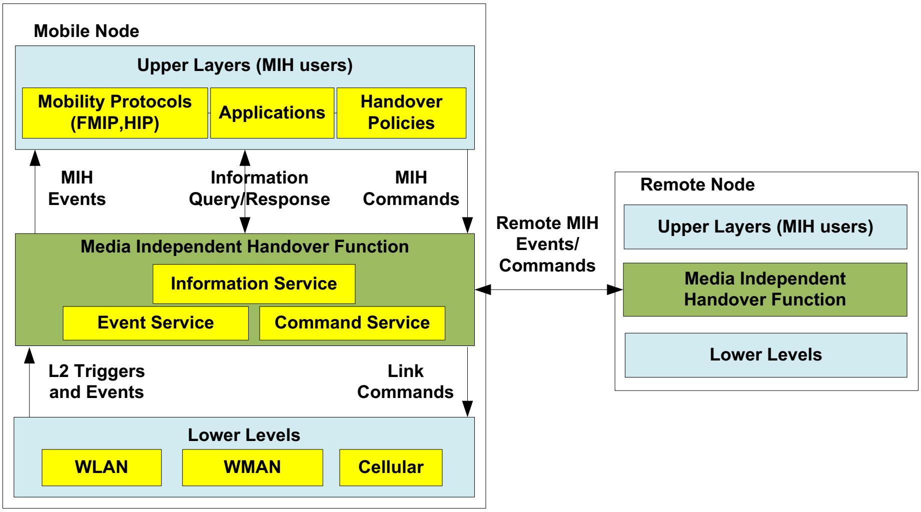


Fig. 1. Media Independent Handover Framework

The Media Independent Event Service (MIES) is a communication procedure where indications for handoff (Events) are passed to the MIH users for further handling. There are two types of Events: Link events and MIH events. The Link events are originating from the Link or Physical layer and can be a change in the state of the parameters of these layers or statistical information. MIH events are Link layer events that are received from the MIHF and are either propagated to the MIH users or to a remote MIH entity.

The Media Independent Command Service (MICS) provides a set of handover commands in order for the MIH users to be able to implement their handover decisions. The local link commands are received from the MIHF and are being mapped to Link layer commands. Also remote MIH commands are sent through the MIHF to remote MIH entities to enable network or client originated handovers.

The Media Independent Information Service (MIIS) is one of the most important services in the MIH framework. MIIS is a database that contains all the available information about the network ranging from channel parameters to presence of application layer services. It is used by mobility protocols in order to find appropriate networks that can facilitate a handover.

Figure 2 presents two examples of usage of the MIH Framework. In the first scenario, the mobile user wants to start a video session and makes use of the MIIS in order to find the appropriate network that guarantees the desired QoS. In the second scenario MIH with information such as current received signal strength and geographical position handovers the mobile node in order to preserve his/her VoIP session while it is moving out of the range of the WiFi network.

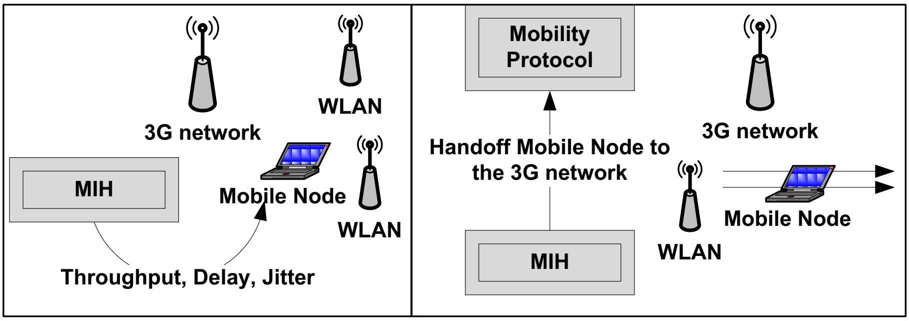


Fig. 2. MIH Framework Example Scenarios

3 Design and Implementation of the Experimental MIH Platform

3.1 Experimental Framework

Our experimental platform based on MIH (Fig. 3) consists of two WiFi networks and one virtual 3G network. Each access network experiences different network load over time. The mobile node that is in the coverage of these wireless networks starts a video session with the video server by selecting randomly one of the network. During the streaming session, events (handover indications), are collected from the MIH server which contains the handover decision and initiation modules (target radio access network). These modules compare this information with predefined thresholds to handover the client to the best network (Network Originating Handover). Test cases will be executed both with the MIH server enabled and disabled in order to evaluate the impact of MIH on the perceived video quality.

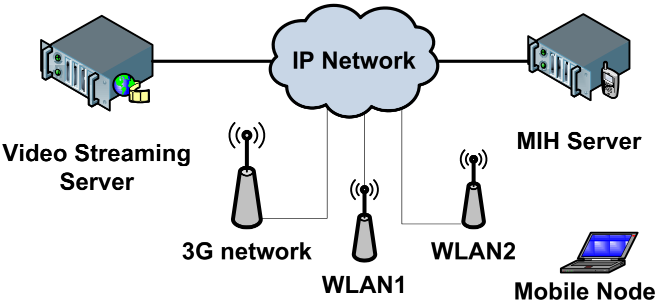


Fig. 3. Design of the Experimental Platform

3.2 MIH Framework

The MIH Server in the platform (Fig. 4) collects packet loss events (link 1) from the available wireless network as well as from the current session of the video client.

The handover mechanism is a part of the centralized architecture 3 and consists of the following steps:

1. **Handover decision:** A handover module is responsible to collect statistics from the MIES from both mobile terminal and radio access networks (SNR, packet loss). The monitored MIH parameters will be evaluated and compared against a set of predetermined threshold values. These thresholds are either determined be the network provider and are specified in each user's profile.
2. **Handover initiation:** When one or more threshold values are violated, the MIH initiation module is responsible of finding the best wireless network that can facilitate the current video service; this is done by comparing the packet loss metrics of every wireless network that are found at the MIH Information Service (MIIS) with the predefined thresholds. When the best network that fulfils the conditions is found, the Handover Initiation Module sends a handover Execute command (link 2) with the old and the new IP address to the Mobility Protocol.
3. **Handover execution:** The final stage is the execution of the vertical handover to the decided neighbouring network. The Mobile IP platform is responsible of handling the vertical handover and of ensuring seamless service continuity. For Simplicity, we have emulated a Mobile IP protocol by adding a handoff delay (Home Agent Registration and Route Optimization) that corresponds to the latency experienced in a real environment 7. With this module the video server upon the receipt of the handover execute command routes the traffic to the new IP address for having a seamless handover.

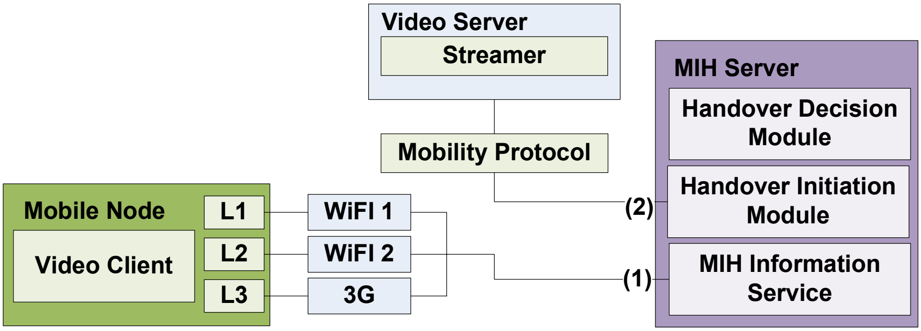


Fig. 4. MIH Design of the Experimental Framework

3.3 Network Load at the Radio Access Networks

In a testing environment it is necessary to find ways of introducing packet loss or traffic to the connections so that handover decision is triggered.

The background traffic at each radio access network has been emulated by a Markov chain. Without loss of generality, the background traffic will be emulated as multiplexed video traffic from N homogeneous video sources. The most important statistical characteristic in a single video source is the degree of correlation between adjacent frames is based on a 3-state Markov chain represents not only correlation between frames of the same type, but of different type as well 8. The scene detection algorithm which is applied in order to distinguish statistical scene changes is based on the measurement of significant changes in the sizes of two consecutive GOPs 9. The statistical scene change in an MPEG coded video may occur at any frame type 10. The two conditions that need to be satisfied together are:

$$\frac{\left|GOP(n+k+1)-GOP(n+k)\right|}{\frac{\sum_{j=n}^{n+k} GOP(j)}{k+1}} > T_1 \tag{1}$$

$$\frac{\left|GOP(n+k+2)-GOP(n+k)\right|}{\frac{\sum_{j=n}^{n+k} GOP(j)}{k+1}} > T_2 \tag{2}$$

Where GOP(n), n=1,2,3,… is the nth GOP size and T1 and T2 are thresholds that depend on the specific characteristics of the video. If the nth GOP is the initial GOP of the i-th scene, and the above conditions are satisfied, then the (n+k)th GOP is the last GOP of the i-th scene and (n+k+1)th GOP is the starting GOP of the (i+1) scene. The K states within the Markov chain represent the scene changes, where each scene is allocated to the appropriate state. It has been found that the pdf distribution of the states follows the gamma distribution 7, 10. The number of states K has been decided according to the following formula:

$$\begin{gathered}\frac{\text{max\_scene\_frame\_size-min\_scene\_frame\_size}}{\text{K-1}} = \text{step} \\ \left\lceil \frac{\text{average\_scene\_frame\_size-min\_scene\_frame\_size}}{\text{step}} + 1 \right\rceil = \text{state\_number}\end{gathered} \tag{3}$$

Assuming that the scene state at the n-th frame time is S_n then the transition probabilities from one scene state to another in the state transition diagram, are defined as follows:

$$\begin{gathered}p_{i,i} = P\left(S_{n+1}=i \middle| S_n=i\right) = \frac{Nf_i - Ns_i}{Nf_i} \\ p_{j,i} = P\left(S_{n+1}=j \middle| S_n=i, j^1 i\right) = \frac{Ns_{ij}}{Nf_i}\end{gathered} \tag{4}$$

Where, $p_{i,i}$ is the probability that the next frame will belong to the same scene state i as the current frame. Additionally, $p_{i,j}$ is the probability that the next frame will belong to state j when the current frame belongs to scene state i. Nf_i and Ns_i are the total number of frames and the total number of scenes in scene state i respectively. Finally, Ns_{ij} is the number of scene changes from state i to state j. The above statistical model represents video traffic from a single MPEG-4 video source. In order to generate video traffic in a radio-access network, several homogeneous and mutually independent statistical video sources have been used. Thus, the aggregate video traffic model can be obtained by creating multiple instances of the single traffic model 11.

$$P_{loss} = \frac{\sum_{t}\left(\sum_{i=1}^{K}\sum_{j=1}^{N}\hat{I}+\hat{B}+\hat{P}-C_{k}\right)}{\sum_{t}\left(\sum_{i=1}^{K}\sum_{j=1}^{N}\hat{I}+\hat{B}+\hat{P}\right)} \tag{5}$$

Where, Ploss is the packet loss probability, t is the video transmission time period, $\hat{I}, \hat{B}, \hat{P}$ are the mean frame bit rates of I, B, P frame types, respectively, K and N are the number of scene states and video sources, respectively. Ck refers to the capacity (throughput) of the kth specific radio access network. In the case of WLAN, the throughput has been set to 5Mbps, whereas in the case of 3G throughput has been set to 2Mbps.

4 Test Scenarios and Performance Results

Our experimental platform comprises the following elements: one 3G virtual network and two WLAN APs. Multiplexed video traffic is inserted to each wireless network according to the description of the previous paragraph. Each radio access network is stressed with up to 100% network load of its maximum throughput. This is due to the fact that the platform has been stressed in order to evaluate handover triggering in case of network congestion. Dummynet has been used in order to emulate the packet loss and delay in each radio access network 12. A real-time H.264 video is monitored throughout the experimental seamless handoff process. A long video sequence (2500 frames-PatrasTV YUV video sequence) in QCIF format (176 x 144 pixels) has been used in order to test the MIH. The testing video sequence has been encoded using the H.264/Advance Video Coding reference software from Vanguard Software Solutions 13. The q-step size has been set to 12; the GOP of the encoded video sequence is structured as *IPPPPPPPPPPPIP...*, with an intra-frame period of 12 frames and a *0*-list of reference frames, 5 frames long. When either the monitored instantaneous packet loss of the video session reaches a threshold or the aggregate packet loss at the radio access network exceeds a limit, handover will be triggered by the MIH functionality. During the experimental phase, we have measured the following: RTP throughput, RTP Packet loss and video Y-PSNR of MIH enabled versus MIH disabled handoff scenarios.

The following two figures(Fig 5, Fig 6) illustrate the received RTP Throughput and RTP Packet loss on the client for MIH triggered experiment (it is accomplished by choosing the best available access network in terms of network load) versus MIH disabled (MIP chooses the radio access network in randomly manner by applying network discovery) over time. In the MIH Enabled scenari,o it is clear that the best candidate network is chosen, thus both throughput and packet loss are optimised under certain network conditions. In the MIH Disabled scenario the mobile IP chooses randomly the radio access networks and this leads to sequential improper selections that except the increased packet loss of the new network add additional overhead due to network discovery that leads to high packet loss at the client.

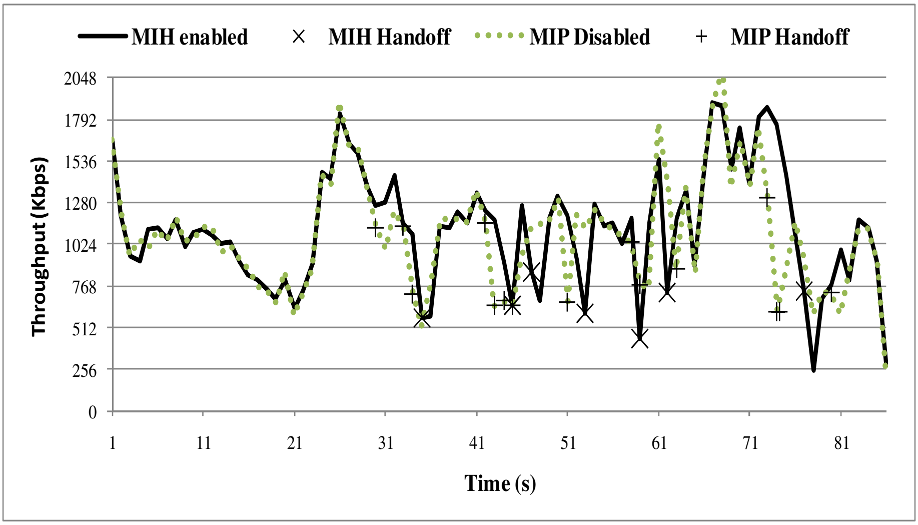


Fig. 5. Client Throughput (MIH Enabled versus MIH Disabled)

Table 1. Average Client Throughput per Test Case

Test Case	Average Throughput (Kbps)
MIH Enabled	1115.72
MIH Disabled	1083.74

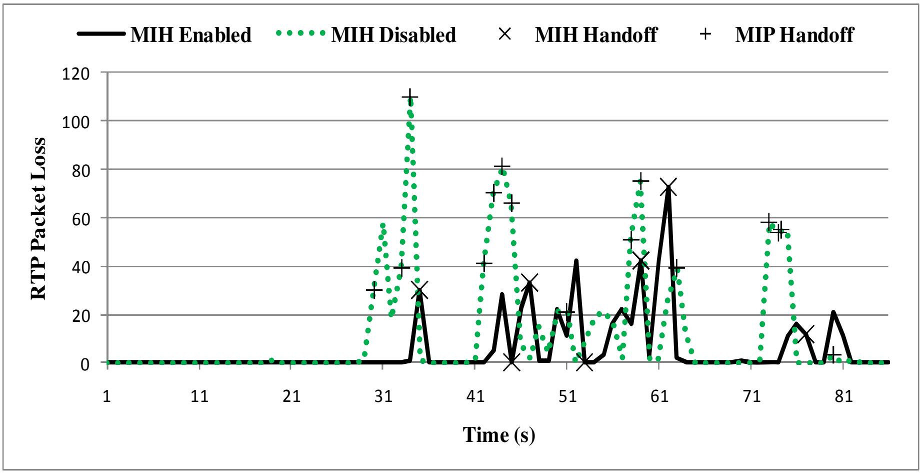


Fig. 6. Client RTP Packet Loss (MIH Enabled versus MIH Disabled)

Table 2. Average RTP Packet Loss per Test Case

Test Case	RTP Loss
MIH Enabled	2.7%
MIH Disabled	5.7%

The following figure (Fig 7) shows the perceived video quality on the client. In the MIH Disabled scenario the video quality drops suddenly 10.9 dB for a long time period (28 – 35 second) due to three sequential improper handoffs. In the scenario where the MIH framework is used the video quality is maintained to acceptable levels by handing over always to the best candidate network.

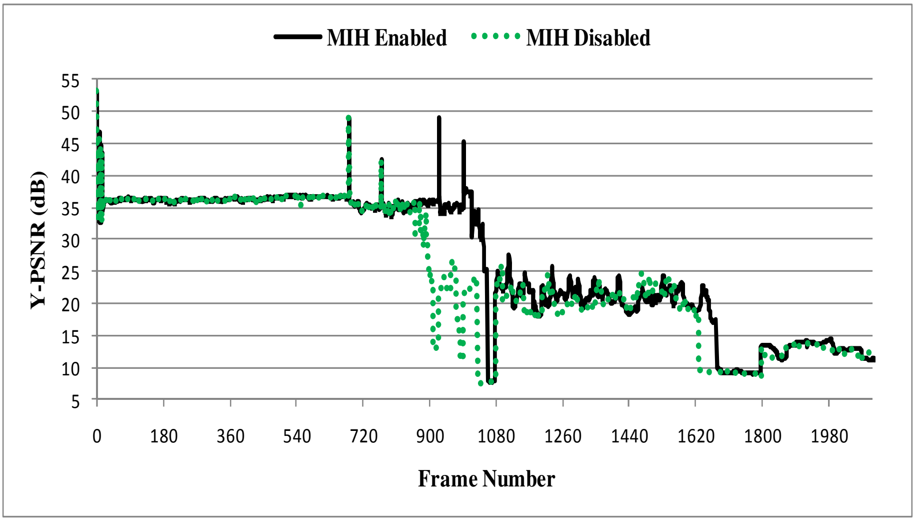


Fig. 7. Video Y-PSNR (MIH Enabled versus MIH Disabled)

Table 3 illustrates the average PSNR of the MIH enabled versus the MIH disabled scenario, throughout the experiment. It has been show that the average Y-PSNR is improved by a factor of 1.09dB.

Table 3. Average Video PSNR and MIH Delay per Test Case

Test Case	PSNR (db)
MIH Enabled	24.59
MIH Disabled	23.50

Finaly Figure 8 and Figure 9 depict the video frame loss per handoff over time. Due to the fact that network discover procedure in Mobile IP adds significant delay overhead, the percentage of frame loss in MIH disabled scenario is higher than that of MIH enabled scenario. Table 4 illustrates the average Frame Loss, where the average loss in MIH disabled is 8% higher than MIH enabled.

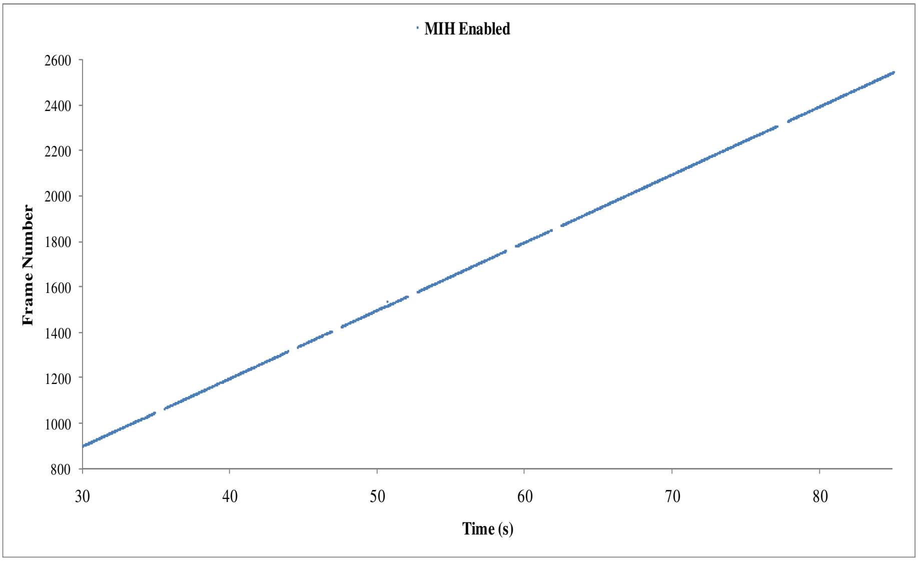


Fig. 8. MIH Enabled Frame Number/time

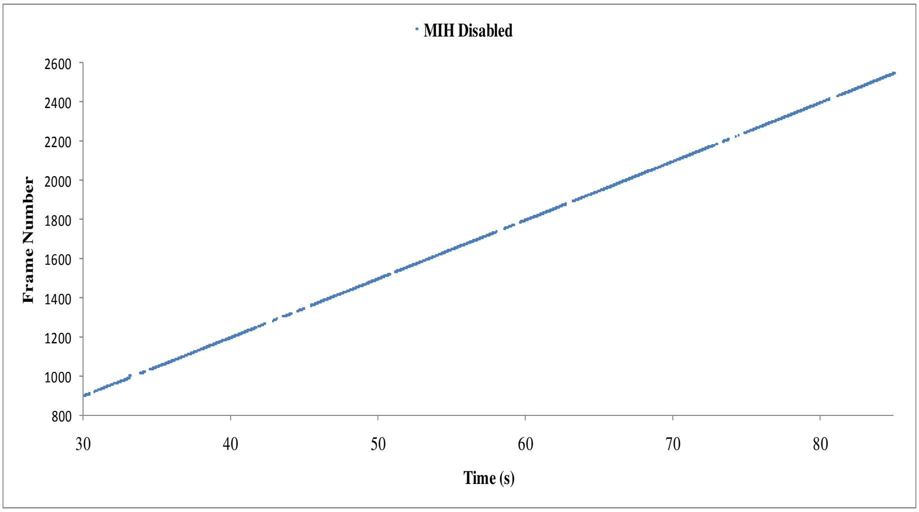


Fig. 9. MIH Disabled Frame Number/time

Table 4. Average Frame Loss per Handoff per Test Case

Test Case	Average Frame Loss per Handoff
MIH Enabled	18
MIH Disabled	26

5 Conclusions

This paper presents an experimental platform for video streaming services across heterogeneous radio access technology networks. The MIH platform collects statistics from the both network layer and physical layer. In the proposed MIH platform, triggers from the network layer have been studied from both the network and the mobile terminal. When packet loss reaches a threshold, handover is initiated and MIH selects as candidate radio access network, the least congested. It has been shown that MIH maintains the video quality of an on-going session by selecting the least congested radio access network. Through experimentation MIH-enabled handover improve substantially perceived video quality against MIH-disabled handover.

Future steps, include on the fly adaptation of video session in case that the mobile node should handover in a radio access network with limited bandwidth, use of estimation methods by determining the level of packet loss that is due to physical impairments from that that is due to network congestion and use of network metrics within a time window in order to estimate its status.

References

1. Ekstrom, H., et al.: Technical solutions for the 3G long-term evolution. IEEE Wireless Communications Magazine 44, 38–45 (2006)
2. Foldor, G., Eriksson, A., Tuoriniemi, A.: Providing Quality of Service in Always Best Connected Networks. IEEE Communications Magazine 41, 154–163 (2003)
3. Rodriguez, J., Tsagaropoulos, M., Politis, I., Dagiuklas, T., Kotsopoulos, S.: A Middleware Architecture Supporting Seamless and Secure Multimedia Services across an Inter-technology Radio Access Network. IEEE Wireless Communications Magazine 16, 24–31 (2009)
4. IEEE 802.21/D10.0. Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services, IEEE Draft (2008)
5. Lampropoulos, G., Salkintzis, A.K., Passas, N.: Media-Independent Handover for Seamless Service Provision in Heterogeneous Networks. IEEE Communications Magazine 46, 64–71 (2008)
6. de la Oliva, A., et al.: An overview of IEEE 802.21, Media Independent Handover Services. IEEE Wireless Communications Magazine 15, 96–103 (2008)
7. Xie, G., Chen, J., Jianhua, H.Z., Yu Zhang, Y.: Handover Latency of MIPv6 Implementation in Linux. In: IEEE Global Telecommunications Conference, Washington, DC, USA (2007)
8. Dai, M., Loguinov, D.: A unified traffic model for MPEG-4 and H.264 video traces. IEEE Transactions on Multimedia 11, 1010–1023 (2005)
9. Yoo, S.-J., Kim, S.-D.: Traffic modeling and QoS prediction for MPEG-coded video services over ATM networks, using scene level statistical characteristics. Journal of High Speed Networks 8, 211–224 (2000)

10. Krunz, M., Tripathi, S.: Scene-Based characterization of VBR MPEG-Compressed video traffic, Technical Report TR-3573, Institute for Advance Computer Studies, Dept. of Computer Science, University of Maryland (1996)
11. Politis, I., et al.: On the QoS Assessment of Video Sessions in Heterogeneous 3G-WLAN Networks with Seamless and Secure Mobility Support. China Communications Magazine 4, 105–119 (2007)
12. Rizzo, L.: Dummynet: a simple approach to the evaluation of network protocols. ACM SIGCOMM Computer Communication Review 27, 31–41 (1997)
13. Vanguard Software Solutions, `http://www.vanguard.com`

A Lightweight Macro-mobility Framework

Karel De Vogeleer, David Erman, Markus Fiedler, and Adrian Popescu

Blekinge Institute of Technology, Karlskrona, Sweden
{kdv,der,mfi,apo}@bth.se

Abstract. This paper presents the design of a lightweight framework to provide vertical handover for macro-mobility on handheld devices. The framework is designed for mobile-controlled handover and does not require modification of the Internet infrastructure. The framework enables users to control the entire vertical handover process so handover decisions are driven by user preferences rather than ISP considerations. UDP tunneling is used as the basis for seamless roaming. Support nodes participate in mobility management by keeping track of the mobile users. We elaborate on a proof-of-concept implementation targeted to be deployed on the Android platform.

Keywords: Vertical Handover, Always Best Connected (ABC), Multihoming, Seamless Roaming, Mobility Management.

1 Introduction

Mobility is one of the prominent factors that describe computer devices today. Moreover, mobility in wireless networks becomes increasingly popular especially with the introduction of smart phones. Market studies show that the market share of smart phones continuously increase even in times of economic crisis.

In this paper we suggest a seamless handover framework that enables mobility for users from one network to another. *Multihoming* is an important prerequisite in our framework, *i.e.*, maintaining multiple interfaces or connections over which Internet Protocol (IP) based communication is enabled. 3G, WLAN and fixed Ethernet are well-known examples of IP based substrates. *Multihoming* together with our framework enables users to participate in *seamless handover*. *Seamless handover* is defined as a handover in which no change in service capability, security, or quality is noticeable [10]. We refer to *vertical handover* when migrating from one technology to another. Networks accessed through these technologies can be administrated by different domains. The reason for conducting a vertical handover is usually to improve Quality of Experience (QoE) towards users or to maintain connectivity. Efficient network selection, security, flexibility, transparency with reference to access technologies and provisioning of Quality of Service (QoS) are the most common parameters taken into account when performing handovers. This paper, however, does not cover the decision making process for adequately deciding when and where to perform a vertical handover.

We differentiate between *proactive* and *reactive* handover. *Proactive* handover is used when referring to handovers completed before network connectivity is

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 567–578, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

lost. The initiating trigger is usually generated by a mechanism employing artificial intelligence , typically a decision engine. *Reactive* handover occurs when connectivity is lost and, as an attempt to re-establish connectivity, a vertical handover is initiated. Proactive handover is not always possible in unpredictable circumstances, *e.g.*, weak signals while driving through a tunnel. Proactive algorithms are also known as Make-Before-Break (MBB) whereas reactive algorithms are referred to as Break-Before-Make (BBM). Proactive handover is thus better suited to support seamless mobility than reactive handover.

The most known mobility frameworks developed by the IETF are Mobile IPv4 (MIPv4) [13] and Mobile IPv6 (MIPv6) [6]. Unfortunately, MIPv6 is not adequate to support fast handover [7] and MIPv4 is not widely deployed even though it was initially proposed in 1996 [12]. Moreover, in the 90's numerous network architectures for mobility support were proposed. Yet almost 20 years later, Internet Service Providers (ISPs) seem reluctant to adopt mobility features in their infrastructure. Possible reasons for this are that they are not willing to invest additional money to extend their infrastructure, no commonly accepted standard for handover is yet defined or the fear of losing costumers to other ISPs. Also the diversity of existing access networks, the lack of interoperability of vendor equipment and the lack of techniques to measure and assess the performance challenge handover solutions. The adoption reluctance of ISPs is a good motivation to look for alternative mobile-centered handover solutions if we want to benefit from mobility today.

Limitations must be solved in order to support mobility in the TCP/IP protocol stack. These limitations include incorporation of cross-layer cooperation and awareness of concerned layers with regards to mobility. For example the congestion control mechanism in TCP is inadequate to perform well in mobile environments. The mechanism is unable to differentiate between packet loss as a result of link properties or as a result of handover performance degradations. Also, improper design of applications towards mobile environments contribute to mobility issues.

Vertical handover solutions can be classified in several ways [10]. One approach is to divide the solutions from the point of view they tackle the problem, *i.e.*, from the user's or the network's point of view. User-centric, or mobile-controlled, handovers have the advantage that the user has full control over the handover mechanism. Network-controlled handovers are usually faster in signaling, *e.g.*, because of traffic prioritization abilities, and place a smaller burden on the mobile device's resources. Vertical handover frameworks can also be divided into three other groups: handover in homogeneous, heterogeneous and IP-backbone networks. While the efforts done by IEEE focus on the first two groups, the third group is where the Internet Engineering Task Force (IETF) is active. The 3rd Generation Partnership Project (3GPP) provides a unified mobility concept that primarily focuses on QoS support and MBB handover. Special Working Groups (WGs) are also active within the IETF, which focus on auxiliary enhancements for mobility support.

Furthermore, solutions can also be classified according to their situation in the Open System Interconnection (OSI) reference model. The most notable vertical handover solution on the Data Link Layer is put forth as the IEEE 802.21, which is known as the Media Independent Handover (MIH) framework for seamless handover in heterogeneous networks [5]. MIH provides a framework pertaining methods and procedures for managing handovers irrespective of media. Mobile nodes and the network collect measurements that are used to make handover decisions. The MIH core exposes its facilities as an Application Programming Interface (API) to higher layers. The unified interface is intended to work on any access technology. The framework presented in this paper fits the view of the MIH core.

Overviews covering existing vertical handover frameworks and mechanisms can be found in [1,2,9] and others.

The remainder of the paper is organized as follows: we define the requirements of our framework in section 2 and the architectural design of our framework in section 3. Section 4 reports on the current status of our implementation efforts. We conclude the paper in section 5, where we state our future actions and present the conclusion of this paper.

2 Handover Requirements

The vertical handover framework presented is part of PERIMETER, a STREP project granted by EU FP7. PERIMETER's main objective is to establish a new paradigm for user centricity in advanced networking architectures [11]. PERIMETER approaches the seamless mobility problem from a user-centric perspective point of view. Therefore seamless mobility can be achieved by actual user needs rather than business considerations. By deploying the vertical handover architecture we provide PERIMETER a framework for "Always Best Connected (ABC)" in a multiple-access multiple-operator environment.

Transparency, user-centricity and deployability on handheld devices are the needs of PERIMETER and thus for the framework. Transparency has a two-fold meaning in the sense that the framework must be transparent for applications, so legacy applications are able to use the framework. This introduces an extra level of complexity. Also, the framework must be transparent to the end-user. The framework is not supposed to drain resources of the device that it operates on. Although handheld devices become more powerful, resources as battery life, bandwidth and computational power are limited. When we take these requirements into account, we are limited to certain solutions. Because of the mobile-controlled handover feature of the framework we must minimize the dependency on the Internet infrastructure. Well-known and studied handover technologies, *e.g.*, MIPv4 and 3GPP, thus do not fit our requirements. As a result, a software-based solution is needed.

The main difficulty in vertical handover lies in the fact that commonly used connection-oriented network protocols, *e.g.*, Transmission Control Protocol (TCP), are not designed to deal gracefully with mobile environments. A connection in TCP is defined as the sender's and receiver's IP address and port pair. If one of these duplets change during the communication, the connection will fail. This might even happen during vertical handovers. Port numbers are not likely to change during handovers as opposed to the IP address. The current Internet architecture does not allow migrating from one technology to another, neither intra-domain nor inter-domain, retaining the same IP address in networks when MIPv4 or MIPv6 are not enabled. A system is therefore desired by which the end-user can easily swap interfaces, *i.e.*, IP addresses, without interrupting ongoing services. This is contradictory to the idea of fixed interfaces used in connection-oriented transport layer protocols. These protocols were originally designed without the consideration of mobile environments. A solution can be to deploy a transport protocol that can cope with mobile environments, *e.g.*, Stream Control Transport Protocol (SCTP). Yet when one must support legacy applications, changing the transport layer protocol is challenging.

Furthermore, the framework must be able to cope with Network Address Translations (NATs), Port Address Translators (PATs) and firewalls. Telecom companies and ISPs use NATs and PATs technologies throughout their networks and retail products. A part of these only seem to cope with UDP and TCP connections. For ISPs it is also usual to allow only communication emanating from within their networks. This is a severe impediment for pure Peer-to-Peer (P2P) technologies. All these limitations create a complex environment for designing a straightforward handover framework.

3 Architectural Design

We now describe the architectural design of our macro-mobility vertical handover framework.

A virtual fixed network is created on top of the existing communication channels to provide (legacy) applications a fixed point to which they can *bind* to. Applications are connected to the virtual network through a virtual interface. The virtual interface has a fixed IP address that does not change during the uptime of the device. This is in contrast with network interfaces that can come up, go down and change IP address on-the-fly in mobile environments. The concept of virtual interfaces are well known and used. A popular implementation is, *e.g.*, the TUN-TAP driver used in for example the VPN project OpenVPN [3]. We can only operate the virtual address when both communication ends are using and maintaining the virtual address space. Traffic going through the virtual interfaces without any additional measures are however invalid on the Internet. We therefore tunnel the traffic going through the virtual network devices over real interfaces. A tunnel virtually connects two end-nodes in such a way that they perceive they are physically connected to the same network. Seamless roaming or seamless mobility is then achieved by transmitting the tunneled data over one of the physical interfaces. This action alters the tunnel header, yet it does not change the data encapsulated by the tunnel.

The proposed framework utilizes User Datagram Protocol (UDP) tunneling. UDP packets are prone to vertical handover, NATs and PATs are able to cope with them.

Tunnels have also drawbacks; the introduction of extra computational overhead and the extension of packet headers and results in less data per PDU. For UDP tunnels each data unit is preceded by an additional IP header (20 B minimum), UDP header (8 B), and a tunnel header. The size of the latter is arbitrary. Our framework uses this space for QoS measurement purposes on the tunnels. Furthermore, performing a vertical handover on the same access technology between two different networks is impossible without interrupting the service.

3.1 Roaming Strategies

Seamless roaming is achieved by means of tunneling data. Tunnels can be created, deleted and relayed, henceforth referred to as operations. The roaming strategies apply to all tunnel operations and how tunnels are managed and data is multiplexed into tunnels. We differentiate between four different roaming strategies:

- *Destination-oriented strategy*: tunnels are created per destination. All outgoing data is grouped per destination and sent over the appropriate tunnel that leads to the destination. Tunnels are deleted when the destination of the tunnel disconnects or the tunnels are unused for a predefined amount of time. This strategy has limited flexibility when it comes to service and application differentiation. Only per-destination QoE can be targeted.
- *Application-oriented strategy*: data is assigned to a tunnel per application. Data from multiple applications are treated separately but can be sent over the same tunnel. Similarly, relaying connections happen per application. Even though this strategy might introduce duplicate tunnels to destinations, it is possible to provide application-differentiated handover. This means concretely that the QoE per application can be maintained.
- *Protocol-oriented strategy*: tunnels are created per protocol, *i.e.*, data is bundled per protocol and then tunneled to its proper destination. Transport layer protocols as well as application layer protocols are taken into account by the protocol-oriented roaming strategy. The protocol-roaming strategy offers the advantage to handover protocol streams independent of where the data emanates. Thus the protocol-oriented roaming strategy is able to provide protocol differentiation.
- *Service-oriented strategy*: data is treated in this case per service. To enable this, an extra level of information is needed to identify particular data as a specific service. In this strategy data is bundled per service and multiplexed into the proper tunnels. As a result QoE per service can be maintained.

The vertical handover framework presented in this paper currently utilizes an application-oriented strategy. This strategy has the most straightforward implementation. An application is bound to a socket and usually does not share the socket among others. Traffic emanating from a particular socket is then handled as per each application's preference.

3.2 Mobility Management for PERIMETER

Mobility Management is a very important issue in mobile environment. In extreme cases, a small physical movement can result in a change of network connectivity. Hence the user might disappear and appear somewhere else in the network landscape. As a result the physical IP address will change. Unpredictable changes of physical IP address makes it difficult to locate users. By introducing a third party we can solve this problem. Users report to the third party at which IP address(es) they are available. The third party is henceforth referred to as the *Location Service*. The service has similar functionalities as the Home Subscribers Database (HSS) in the IP Multimedia System (IMS) architecture.

The *Location Service* can be, *e.g.*, a Distributed Hash Table (DHT) in which all mobile nodes are participating or could be implemented as a server operated by a Mobile Virtual Network Operator (MVNO). A distributed network of servers hosted by the mobile users at their home may also provide a solution. Many other configurations are possible.

An entry in the *Location Service* comprises of two compulsory elements and one optional element: a virtual IP address and a physical IP address that the user is reachable at and optionally, a string identifier of the user. The latter can for example be a DNS name or SIP identifier. Users in the system are expected to keep their entry in the *Location Service* up-to-date. Users report typically their location to the *Location Service* when they boot or turn off their device and after handover.

The flow diagram of the signaling between two PERIMETER enabled nodes is shown in figure 1 and elaborated below. Here we assume that *User A* initiates all operations to *User B*. The *Location Service* supports both peers when needed.

- Setting up a connection to a mobile user means concretely setting up a tunnel. The tunnel set-up procedure starts with retrieving the destination user's entry from the *Location Service*. A request is sent to the destination user to set up a tunnel with given settings. This request can be sent over any available network interface. Once the other side has parsed the request, configured its side of the tunnel and activated the tunnel, the destination sends an acknowledgement back to the initiating user. All messages are sent outside of the tunnels. Upon reception of the acknowledgement, the initiating user activates the tunnel at his side.
- Performing a handover is essentially the relay of a tunnel over another physical interface. The relay of a tunnel is achieved by creating a second tunnel. All traffic is forwarded into the new tunnel and the old tunnel is removed. The main concern in the relay of tunnels is the prevention of data loss. Data might be residing inside the old tunnel when it is being shut down. The reachability of the other side must be maintained during handover for signaling and data exchange. To address the latter the handover must be carried out as fast as possible. For *proactive handover* the handover must be initiated at the right point in time before connectivity vanishes completely. To circumvent the data-loss problem the old tunnel is only deactivated when the new tunnel is configured and running. In case of *reactive handover* data

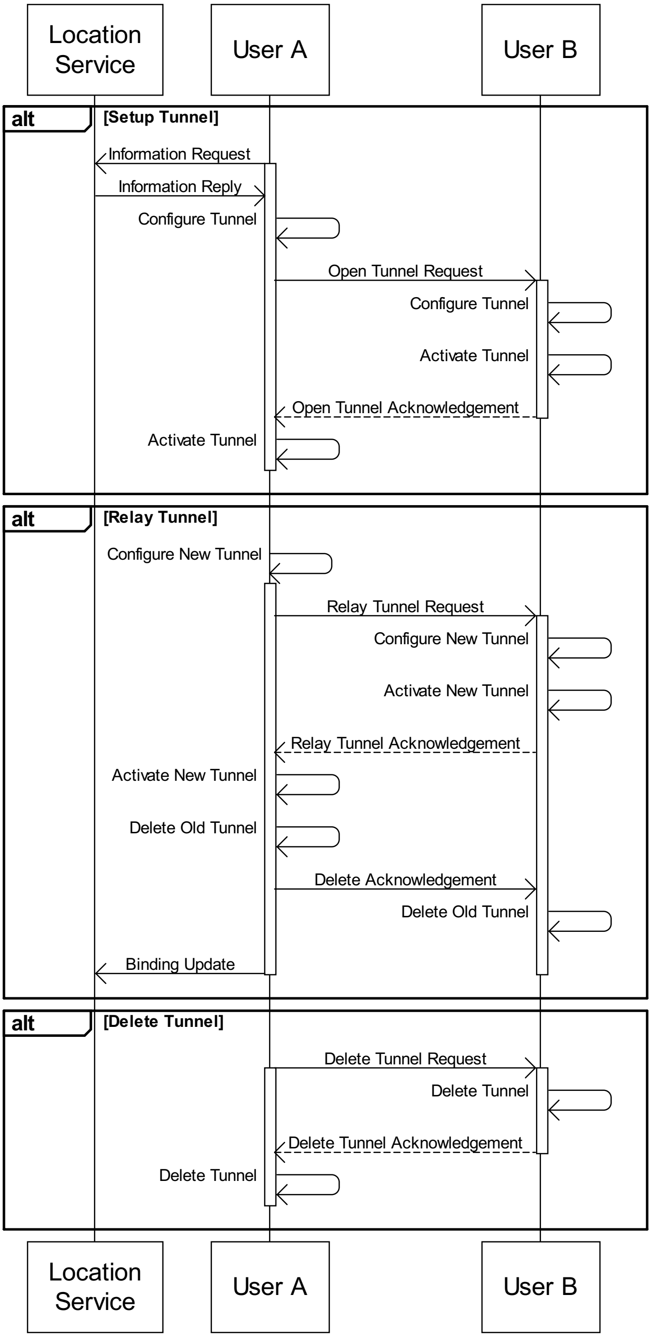


Fig. 1. Signaling scheme between the location service and mobile users operating the vertical handover framework

that is queued for sending is buffered while a new communication channel is being set up.

- Finally, tunnels are deleted when they are not being used anymore or when the destination or source user disconnects. The principles of data-loss discussed above applies to deleting tunnels as well. We do not want to loose data that might still reside in the tunnel upon deletion. Therefore we only tear down the tunnel when we are sure that both sides of the tunnel are fully aware of the operation.

The structure of the control messages are presented in the following enumeration. *Control messages* are exchanged during an operation request described above. *Acknowledgements* are used to confirm or reject a previously received *operation request*. For the operations and acknowledgements, the content of their message body have a common structure containing the following fields:

1. sender-ip: sender's virtual IP address;
2. receiver-ip: receiver's virtual IP address;
3. tunnel-id: Universal Unique ID (UUID) to identify the tunnel [9];
4. seq-number: sequence number of the message;
5. operation: operation to be performed [set-up, delete, relay, acknowledge].

The following fields are appended for operation requests only:

1. sender-ip: sender's physical IP address;
2. receiver-ip: receiver's physical IP address:
3. sender-port: sender's port number;
4. receiver-port: receiver's port number.

Two additional fields are appended for acknowledgement messages:

1. ack: status of request [accepted, rejected];
2. error: reason for acceptance or rejection (optional).

3.3 Architecture of the Handover Framework

The Vertical Handover Architecture describes the design of the framework and is depicted in figure 2. The framework comprises five concrete blocks: the *Tunnel Farm* and *Mobility Manager*, the *Vertical Handover Manager*, the *Network Interface Manager* and the *Tunnel Catcher*. Additionally, a dedicated interface is exposing the frameworks functionalities to the outside world and an interface is assisting network interface calls. The Vertical Handover framework is a passive element in the sense that it only acts upon external triggers, *i.e.*, no internal event generators are present.

Tunnel Farm: The *Tunnel Farm* is an entity that maintains a set of UDP tunnels. The farm's duties are to create, delete and relay tunnels. These three operations together with the intelligence implemented in the *Vertical Handover Manager* provide seamless handover. The operations on tunnels are triggered by different events:

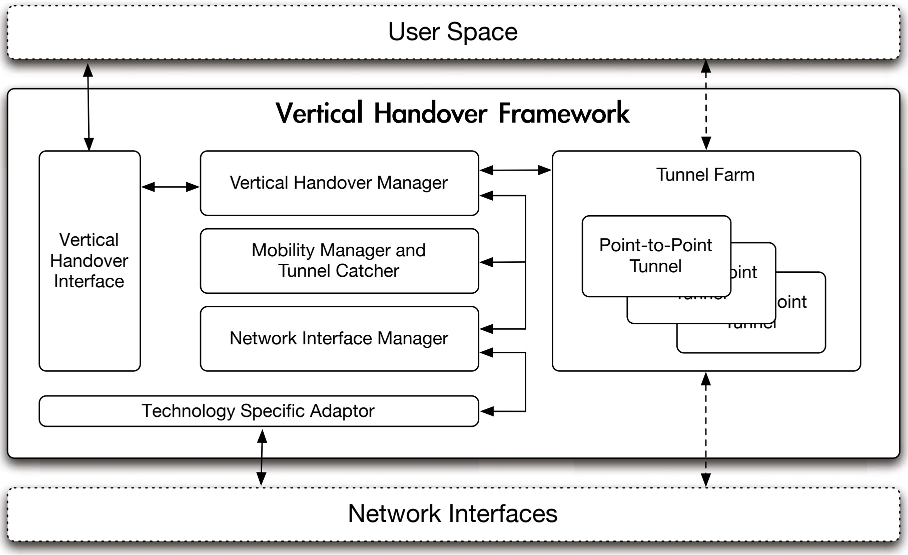

User Space
Vertical Handover Framework
Vertical Handover Interface
Vertical Handover Manager
Mobility Manager and Tunnel Catcher
Network Interface Manager
Technology Specific Adaptor
Tunnel Farm
Point-to-Point Tunnel
Network Interfaces

Fig. 2. Block diagram of the vertical handover framework. Solid lines represent control message flows whereas dashed lines depict user data flows.

- Creating Tunnels: tunnels are created when data is about to be sent or when data is about to be received. This is a critical operation, as data cannot be sent before a tunnel is established at both sides of transmitter and receiver. Therefore, a queue must be implemented to temporarily buffer data until the tunnel is completely initialized. The *Tunnel Catcher* implements a mechanism that detects incoming tunnels and outgoing data. When such an event occurs the data is buffered and the *Vertical Handover Manager* will direct the configuration of a new tunnel.
- Deleting Tunnels: when tunnels are not being used they are deleted. Either a timer expiration or a protocol connection closing signal can be the trigger to delete a tunnel.
- Relaying Tunnels: tunnels are only relayed on demand by the *Vertical Handover Manager*. Though, relaying is in essence a combination of creating and deleting tunnels. Therefore the tunnel relay operation is transparent to the *Tunnel Farm* as creating and deleting tunnels is directed by the *Vertical Handover Manager*.

Vertical Handover Manager: The vertical handover procedures requested by any concerned instance is directed by the *Handover Manager*. The manager decomposes the handover commands and delegates the work to the other blocks in the framework. Communication between these blocks is relayed through the Vertical Handover Interface.

Tunnel Catcher: A negotiation must be held between the users who want to set up a communication channel over the mobility framework. The negotiation pertains the configuration settings of the tunnel, in particular the entry point and the exit point of the tunnel. Therefore a binary signaling protocol is deployed to serve as a communication substrate between mobility aware users and central administrative instances, *e.g.*, the *Location Service*. The *Tunnel Catcher* manages the signaling protocol and cooperates with the *Tunnel Farm* that maintains the tunnels. Communication with the *Tunnel Farm* happens through the *Vertical Handover Manager*.

When switching from one interface to another, *i.e.*, during handover, network addresses change. To avoid connection problems the UDP protocol is used to communicate between handover frameworks. Using UDP avoids delays in connection set-ups, *e.g.*, as induced by TCP, that might affect the seamlessness of the handover.

If, during handover signaling, a request is not replied or acknowledged within a specific time frame, the request is assumed to be lost. A retransmission of the request is then initiated. The time frame for retransmission must be short because in order to conduct seamless handover one must react quickly.

Mobility Manager: Responsibilities involve maintaining the node's entry at the *Location Service*. The manager is mostly active during startup and closing of the mobility framework and during handover.

Network Interface Manager: All network interfaces are managed by the *Network Interface Manager*. Its duties are, *e.g.*, bringing interfaces up and down, configuring interfaces, logging into networks etc. These actions are technology-specific, and therefore, the *Network Interface Manager* relies upon the facilities offered by the *Technology Specific Adaptors*.

Technology Specific Adaptor: The *Technology specific adaptor's* responsibility is translating common operations offered by access technologies. A common API is exposed so that the vertical handover framework can communicate with all interfaces in a unified manner.

Vertical Handover Interface: User-space utilities to configure the behavior of the handover system can communicate with the framework through the *Vertical Handover Interface*.

4 Implementation

The current implementation of the framework is designed to run on a Linux machine with special focus on Google's Android [4] platform. The motivation is that the operating system is accessible, *i.e.*, has an open-source network stack to implement our framework, and the operating system is Linux based. Android also provides a useful set of tools to manage the handheld devices resource's.

Applications in Android run inside a Dalvik virtual machine, which is based on Java technology. To deploy our framework inside a virtual machine however is not desirable because this would introduce unnecessary process delays and be disadvantageous for the seamlessness of handovers. Therefore we opted to implement the framework mostly in the kernel. This approach minimizes changes to the original path that data would take when traversing the network stack and decreases processing load.

The framework including the virtual interface is implemented as a Linux kernel module. The virtual interface is partly based upon the IPIP tunneling driver. All outgoing traffic passing through the virtual driver is multiplexed into the appropriate tunnel according to the active roaming strategy. Outgoing traffic is also forwarded by the virtual interface to the higher layers in the network stack. Communication between the framework, residing in the kernel, and the controlling process in user-space happens through a UDP socket interface or the `/proc` file system.

Preliminary experimental outputs show that the framework is working properly, though some parts in the low-level code could be optimized to yield better performance, *e.g.*, IP address lookups in tables can be accelerated.

5 Conclusion and Future Work

In this paper we presented a lightweight framework for vertical handover. UDP tunnels are utilized as substrate for vertical handover. When migrating from one technology to another tunnels are relayed accordingly. This does not affect the data that is traveling through the tunnels as these events are transparent to the end-user. We elaborated on implementation and design details and we discussed different strategies in relaying tunnels depending upon the kind of service that is offered towards the user of the mobility framework.

We are currently conducting experiments and assessing the performance analysis. The results will then be compared to other vertical handover frameworks and the findings will be published accordingly.

Furthermore, the current design of the framework is prone to erroneous messages and does not handle wrongly formatted commands very well. These could be emanating from malicious entities and other causes. A simple security mechanism is already present in the control signaling under the form of a sequence number. However this does not exclude any type of attack. Security issues and erroneous messages and commands must be addressed in the future.

Acknowledgement

We would like to thank PERIMETER, a STREP project, granted by EU FP7, and MOBICOME, a EUREKA project, granted by VINNOVA for the funding of our research in vertical handover technologies. We also thank the anonymous reviewers for their valuable input.

References

1. Atiquzzaman, M., Reaz, A.A.: Survey and classification of transport layer mobility management schemes. In: 16th International Symposium on Personal Indoor and Mobile Radio Communications, Berlin, Germany (September 2005)
2. Emmelmann, M., Wiethoelter, S., Koepsel, A., Kappler, C., Wolisz, A.: Moving towards seamless mobility state of the art and emerging aspects in standardization bodies. Springer's International Journal on Wireless Personal Communication–Special Issue on Seamless Handover in Next Generation Wireless/Mobile Networks (2007)
3. Feilner, M.: OpenVPN: Building and Integrating Virtual Private Networks. Packt Publishing (2006)
4. Google (2009), `http://www.android.com/`
5. IEEE: Draft ieee standard for local and metropolian area networks: Media independent handover. P802.21/D8.0 (December 2007)
6. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6. RFC 3775 (Proposed Standard) (June 2004)
7. Johnson, T., Prado, R., Zagari, E., Badan, T., Cardozo, E., Westberg, L.: Performance evaluation of reactive and proactive handover schemes for ip micromobility networks. In: Wireless Communications and Networking Conference, WCNC 2009, pp. 1–6. IEEE, Los Alamitos (April 2009)
8. Le, D., Fu, X., Hogrefe, D.: A review of mobility support paradigms for the internet. IEEE Communications Surveys 8(1-4), 38–51 (2006)
9. Leach, P., Mealling, M., Salz, R.: A Universally Unique IDentifier (UUID) URN Namespace. RFC 4122 (Proposed Standard) (July 2005)
10. Manner, J., Kojo, M.: Mobility Related Terminology. RFC 3753 (Informational) (June 2004)
11. Perimeter (2009), `http://www.ict-perimeter.eu/`
12. Perkins, C.: IP Mobility Support. RFC 2002 (Proposed Standard), obsoleted by RFC 3220 (October 1996), Updated by RFC 2290
13. Perkins, C.: IP Mobility Support for IPv4. RFC 3344 (Proposed Standard) (August 2002), Updated by RFC 4721

Enhanced Localization in Wireless Ad Hoc Networks through Cooperation

Senka Hadzic, Joaquim Bastos, and Jonathan Rodriguez

Instituto de Telecomunicações,
Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
`{senka,jbastos,jonathan}@av.it.pt`

Abstract. Next generation networks consider context information to deliver personalized services, where this context can include positioning information. On the other side, positioning information is relevant to some of the network main functions: geographical routing, network coverage, enhanced security, power saving etc. Therefore determining the position of nodes in wireless networks is pivotal and this paper proposes a cooperative iterative framework to expand the overall localization coverage in an ad hoc wireless network.

Keywords: Positioning, Ad hoc, distance estimation, cooperation.

1 Introduction

All-encompassing wireless networks need to provide personalized services to the end user, guaranteeing overall service availability in a highly dynamic environment. Some of those value added services are delivering specific information to the users relevant to their current locations. The position information of mobile nodes in wireless networks can support location-aware applications (e.g. location-based services like mobile commerce, location based advertising, social networking, tracking, monitoring) to offer flexible and adaptive personal services, but can also improve the network performance through location-based routing, load balancing and coverage management. Radio spectrum and terminal battery are the main constraints in wireless communications. For an efficient use of all the available resources, the position information will help to predict the required resources even in heavily loaded networks.

A straight forward example for the benefit of positioning information for location based radio resource management is shown on Fig 1. We consider a scenario where more than one wireless network provides coverage (in this example Beyond 3G or 4G RAN cell and a WLAN hotspot). The idea is to select one of these networks based on its service, capacity and current load, taking into account user's location and mobility information [1]. If the mobile terminal (MT) is moving slowly along the trajectory, it is reasonable to hand over to a small hot-spot cell, which locally provides significantly higher data rates than the Radio Access Networks (RAN) cells do. For a high MT speed along the trajectory, the time that the user resides in the hot-spot cell area is so short, that the effort for a handover exceeds the achievable gain in data rate. In such a case it does not bring any benefit to hand over to the WLAN hotspot. It is preferred to stay connected to the previous RAN cell (BS1) or hand over directly to BS3.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 579–589, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

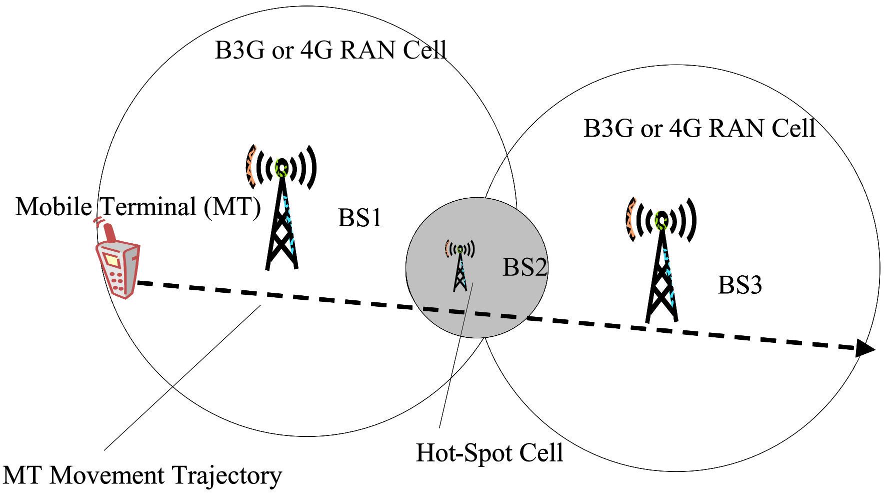


Fig. 1. Location based handover

Global Positioning System (GPS) is the most widely used positioning system. However, it cannot be deployed indoors because of the absence of line of sight transmission between satellite and receiver. GPS receivers are costly and power consuming, which makes them unsuitable in dense ad hoc networks with strict energy constraints. Furthermore, the typical error values for GPS positioning (3-30m) are not tolerable for dense sensor networks. Thus, development of other solutions for indoor scenarios is necessary. In this paper we consider positioning algorithms in ad hoc networks.

Unlike infrastructured networks, ad hoc networks cannot rely on dedicated infrastructure to forward traffic across fixed network segments between mobile users. Furthermore, direct communication between all nodes is infeasible due to limited transmission range. The nodes have to establish multi-hop wireless paths and to cooperate in order to dynamically maintain routes. Cooperation between nodes is essential also for localization, because it allows nodes which are not in range of a sufficient number of references (and therefore at the first sight not able to be localized) to be located. In a two-dimensional space, at least three references are required to estimate a node’s position. Given a limited range, it is very unlikely that a node will be able to directly communicate with a sufficient number of references and estimate its position.

The rest of the paper is organized as follows: the next section describes the key aspects of cooperative localization. Section 3 gives an overview on the state of the art in the area of interest. In section 4 we present our approach to design a new algorithm. The last section, section 5, concludes the paper.

2 Cooperative Positioning

The availability of position information depends on the existing infrastructure, such as GPS satellites or cellular base stations. Cooperative positioning techniques are used in scenarios where non-cooperative (single-hop) solutions are not feasible, or do not perform well in terms of accuracy, availability, cost and complexity. Especially in indoor scenarios, where a line of sight connection to reference nodes is not always available, the mobile terminal can benefit from cooperative positioning in order to obtain information of its own location. Typically, algorithms assume a number of location-aware nodes, called *anchors*. They may have obtained their positions through GPS or by some other means. Those nodes are used as references for the other, unknown nodes to estimate their positions. Generally, the localization process is divided in two phases. The first phase is the ranging phase, where nodes estimate the distances to their neighbors. In the second phase, the ranging information is used for calculation of unknown nodes' coordinates. Optionally, there might be a third phase where the positions are refined through an iterative procedure for further accuracy improvement.

2.1 Ranging Phase

Range measurements can be based on Received Signal Strength (RSS), Time of Arrival (ToA) or Angle of Arrival (AoA). ToA based distance estimation is relying an the fact that radio waves propagate at the speed of light, and knowing the time a signal needs to propagate from one node to another, we can easily obtain the distance between them. Accurate estimates are feasible in line of sight conditions. In order to accurately measure the time of propagation, sender and receiver have to be perfectly synchronized, and therefore fast processing capabilities are needed. One way to avoid the need of precise synchronization is to measure the round trip time (RTT) from transmitter to receiver and back. However, it is still difficult to extract the exact processing and delay time in the receiver. In short range scenarios this value cannot be ignored, as it is in order of transmission time. AoA techniques use antenna arrays to measure the angle at which the signal arrives, but require additional hardware which is costly and needs to be maintained. RSS based methods estimate the distance between sender and receiver by measuring the attenuation in radio signal strength, and considering the appropriate propagation model. In an indoor scenario usually a log-normal shadowing model is being used. The benefit of RSS based location methods is its simplicity and availability regardless the radio access network, as well as the fact that RSS of radio signals is being measured during data communication, to decide whether the packet transmission has been successful or not. There is no additional bandwidth or energy required to perform signal strength measurements. Nevertheless, the performance of these techniques depends on the model used to find the relationship between measured RSS and distance. Moreover, there exist several hybrid approaches that exploit a combination of the aforementioned techniques to enhance localization accuracy and to minimize the number of required reference nodes. Once the distances to a sufficient number of anchors are obtained, a node has to perform a trilateration/multilateration algorithm to compute its coordinates.

2.2 Position Estimation

Lateration uses the geometric properties to estimate the target location. Each estimated distance represents the radius of a circle centered at the corresponding reference node. For 2-D positioning, measurements from at least three reference nodes are

Fig. 2. Trilateration

required, and the location is obtained as the intersection of circles, as represented on Fig. 2.

Having in mind the errors in estimated distances to the anchors, the geometrical trilateration technique can only provide a region of uncertainty [2] instead of a single point. Therefore the solution is based on iterative algorithms to obtain the node position by formulating and solving a set of nonlinear equations. Due to nonlinearity, to find a solution for a (*n*-1)-dimensional system, *n* equations are required. Least Squares (LS) algorithm is used in order to minimize the error between the estimated and the real position. In general, linear LS estimation is a suboptimal positioning technique. However, it has been shown in [3] that it performs similar to the nonlinear ones, especially for small noise variances. Besides that, the computational complexity is significantly lower in linear LS methods. In [4] both linear and nonlinear LS methods for position estimates via trilateration are presented. When distances to more than three reference nodes are available, the technique of position calculation is called multilateration. Here, a position estimate is calculated by reducing the difference between actual distances between node *i* and node *j*, and estimated distances d_{ij}. The difference is given by:

$$f_{ij}(x,y)=\sqrt{(x_j-x_i)^2+(y_j-y_i)^2}-d_{ij}\,. \tag{1}$$

For *n* distance estimates, the position of the unknown node is obtained by minimizing the function

$$F(x,y)=\sum_{i=1}^{n} f_i(x,y)^2\,. \tag{2}$$

2.3 Key Aspects of Cooperative Localization

The main sources of error are measurement errors in the ranging phase, and iterative error accumulation during the second phase. The ranging errors arise due to multipath and shadowing effects. The algorithm should be distributed rather than centralized, meaning it should not depend on one single central point responsible for all computations, due to the infrastructureless nature of ad hoc networks. Additionally, by using decentralized approach the algorithm is tolerant to node failure. To deal with energy constraints, computation and communication overhead should be minimized to save the nodes' battery lifetime. Having in mind that the nodes are in general mobile, the response time should be low, so the localization system can be easily updated every time the topology changes. The algorithm has to provide accurate position estimates, whereby the level of accuracy depends on the application.

Performance parameters are mainly accuracy and latency. Ability to provide low latency is especially important in dynamic scenarios where a low response time is crucial. The two major cost parameters are the amount of communication between nodes, and the computation process in the nodes. Cooperative solutions have to achieve desired cost-performance trade-offs. The number of actively participating nodes should be kept to a minimum, and therefore an appropriate cooperation subset has to be chosen, while the other nodes can be ignored. Such a restrictive and selective use of references is crucial in networks with limited resources.

3 Related Work

In multi-hop scenarios, localization algorithms can be range–based or connectivity-based (also called range-free) [5]. In range-based approaches distance estimates are usually obtained using one of the previously described techniques (TOA, AOA, RSSI). In [6] it has been shown that in multi-hop networks, while increasing the number of hops for a fixed source to destination distance, the accuracy deteriorates for TOA-based systems. In contrast, for RSSI-based systems the accuracy improves. However, most range-based approaches are not suitable for low density networks, since the large distance between nodes does not permit to perform a sufficient number of range measurements. For sparse sensor networks the most widely used technique is multi-dimensional scaling (MDS), a statistical dimensionality reduction technique for data analysis that uses pair-wise distance measurements as input data [7], [8].

On the other hand, range-free algorithms are based on connectivity information among nodes. Two sensors being in range define a proximity constraint, which can be exploited for localization. These approaches do not assume any additional hardware functionality, as they do not rely on distance measurements. Therefore, their main advantage is its simplicity and low cost. In the "Ad Hoc Positioning System (APS)" algorithm developed by Niculescu and Nath [9] anchors flood the network with their locations. The proposed scheme is known in literature as DV (distance vector)-hop. Hops are being counted along the shortest path between any two anchors, to estimate the average distance of one hop. The average hop length is spread through the network as the correction factor. After receiving the correction factor, every node is able to estimate its distance to the anchors and to perform trilateration. The algorithm is completely ad hoc, and does not depend on measurement errors. Simulation results showed the mean positioning error of 45% transmission range.

An extension is the "DV-distance" approach, proposed in [9] where the measured distance is propagated among neighboring nodes instead of hop count. DV-distance is a range-based distributed localization algorithm, using RSS measurements. Performance is comparable to DV-hop, although the method is sensitive to measurement errors. Two similar approaches are the "hop-terrain" algorithm developed by Savarese and Raabey [10], and the "AHLoS" (Ad Hoc Localization System) scheme of Savvides et all [11]. The algorithm proposed in [10] is separated into two phases: start-up and refinement. In the first phase an algorithm similar to DV-hop is used to obtain an initial estimate of node locations. The refinement algorithm is run iteratively afterwards. At each iteration step, all nodes update their location estimates by least squares trilateration, taking into account only nodes within one-hop neighborhood. Refinement stops when, after a number of iterations, the position update becomes small and it reports the final position. It was shown in simulations that the algorithm achieves average position errors of less than 33% of a node's transmission range, when at least 5% of nodes are anchor nodes and the average number of one-hop neighbors is greater than 7 nodes.

AHLoS algorithm [11] uses TOA as the primary ranging method, and multilateration as the basis for position calculation. It follows an iterative scheme: once an unknown node estimates its position, it becomes an anchor and broadcasts its position estimate to all neighboring nodes. The process is repeated until all nodes that can have three or more reference nodes obtain a position estimate (Fig. 3). A drawback of iterative multilateration scheme is the error accumulation that results from the use of estimated locations as anchors. In [12] the authors proposed an iterative algorithm that takes into account the behavior of the channel to provide accurate indoor positioning and importantly reduce error propagation. Simulations showed that inaccurate ranging has a bigger impact on error propagation than the use of estimated (and therefore erroneous) locations as anchors.

Fig. 3. Iterative multilateration

Some algorithms do not perform well in low density networks, for instance those that depend on distance measurements when the transmission range is short. One example is the AHLoS algorithm proposed in [11] that requires a high degree of node connectivity. The percentage of required reference node decreases as the network density increases. A comparison performed in [13] showed that DV-hop requires a minimum connectivity. The refinement procedures are extremely costly in terms of communication overhead since they take many iterations before convergence.

4 Proposed Cooperative Positioning Framework

Aspects that have to be considered when choosing or designing an ad hoc positioning algorithm are limited resources, number and density of nodes, percentage of anchors and network topology. It is also important to choose the appropriate range measurement method for the environment of interest. For example, in high-density sensor networks the most valuable ranging technique is RSS [14]. Limited resources refer mainly to energy constraints in an ad hoc network. The battery lifetime is usually limited, and nodes have low processing capacity. Therefore it is important to have an even distribution of power consumption among nodes, and a distributed approach generally solves this issue. In a purely ad hoc network, not depending on a central server or infrastructure, all of the entities have the same capabilities. The number of actively participating nodes should be kept to a minimum, and therefore a proper cooperation subset has to be selected, while the other links can be discarded.

We propose one algorithm based on iterative multilateration, which provides a way to expand the network coverage in a step-by-step fashion. In this sense, coverage is the fraction of nodes that have an accurate position estimate. We assume a middle-scale ad hoc scenario with a certain percentage of anchor nodes. Specifically, in our simulations we consider 30 nodes, from which 6 are anchor nodes and 24 are unknown nodes. The nodes are placed in a 30m x 30m grid, and transmission range is set to 10 m and 15 m, respectively.

Once a node joins the network, it has to perform some sensing to identify which nodes are in its range. During this network discovery phase, signal strength is being measured to decide whether the packet has been received successfully or not. Therefore we decided to use RSS measurements for distance estimation. We use the log-normal shadowing propagation model, with typical parameters for indoor environment. General expression for this propagation model is:

$$RSS_d = 10\log_{10} P_r = 10\log_{10} P_t - 10\beta \log_{10} \frac{d}{d_o} + X_\sigma , \tag{3}$$

where P_t is the transmitted power, d is the distance between transmitter and receiver, d_o is the reference distance (usually 1m), β is the path loss exponent and X_σ is a zero-mean Gaussian random variable with standard deviation σ, representing the shadow fading component. Typical parameter values for an indoor scenario are $\beta = 3$ and $\sigma = 7$. Once the distances to a sufficient number of anchors are obtained, a node has to perform a trilateration/multilateration algorithm to compute its coordinates. In order to enable 2-D positioning, distances to at least three reference points must be available.

If we integrate message exchanges into routing protocols, location discovery is almost free in terms of communication cost. To choose the nodes most suitable for cooperation, we suggest to associate a utility function to the scenario, as a function of all metrics relevant for the positioning algorithm. This function contains useful information, i.e. which nodes are in range of each other, how is the quality of links between them etc. ‘Quality of link’ parameter is a representation of the channel condition between two nodes in an ad-hoc environment. It helps to establish a statistical measure of the node-to-anchor channel conditions. To assess the quality of links, we perform 100 RSS measurements, and take the statistical mean and standard deviation. Those sets of measurements, related to specific anchor nodes, with a smaller standard deviation are considered to have better quality, and will have a priority in the reference nodes selection phase.

Once the suitable anchor nodes are chosen and the distances to at least three anchors are estimated, position is calculated using least squares. In the first iteration, a node uses anchors as references, and once it calculates its own position, it becomes a new anchor, but with some uncertainty associated with it. This uncertainty of estimate will also be included in the utility function as a metric for reference selection. According to [12], the quality of links is more important for anchor selection than quality of estimate, and therefore it should have a higher priority as part of the utility function. The framework description is given in the following diagram:

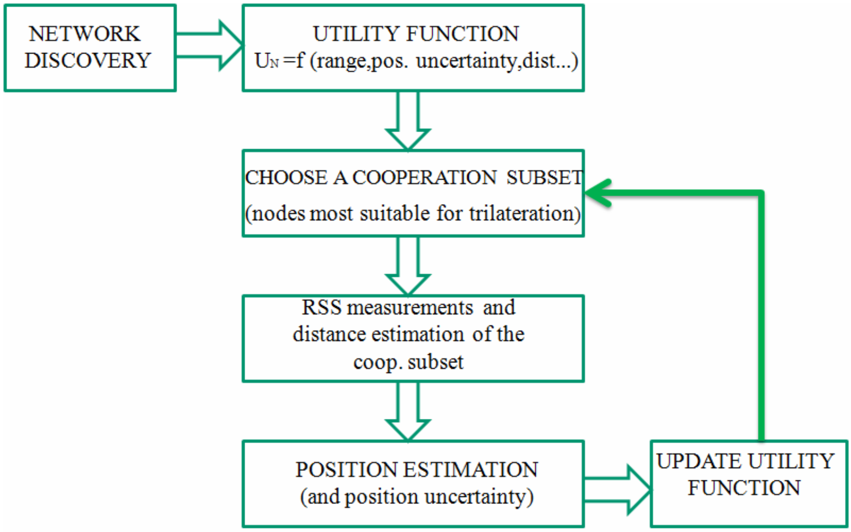

NETWORK DISCOVERY
UTILITY FUNCTION
U_N =f (range,pos. uncertainty,dist...)
CHOOSE A COOPERATION SUBSET
(nodes most suitable for trilateration)
RSS measurements and distance estimation of the coop. subset
POSITION ESTIMATION (and position uncertainty)
UPDATE UTILITY FUNCTION

Fig. 4. Iterative cooperative positioning algorithm

Every newly estimated position acts as a reference point for its neighborhood and extends system coverage. To decide whether or not a new estimate can advertise itself as an anchor, we need to set an error threshold. Threshold adjustment makes it possible to find a trade-off between desired accuracy and number of iterations needed for full coverage. It is evident that communication range will have an impact on coverage. Fig. 5 shows that for a larger range it will be possible to incorporate more new anchors after the first iteration.

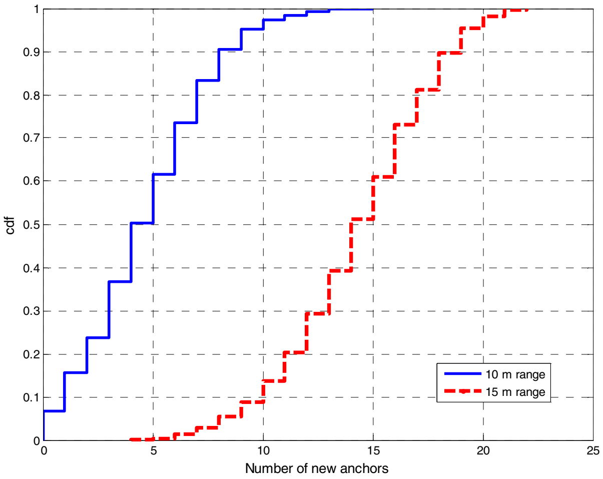


Fig. 5. Number of newly incorporated anchors after first iteration

Fig. 6 plots the error cumulative distribution function (cdf) for transmission range values 10 m and 15 m, respectively.

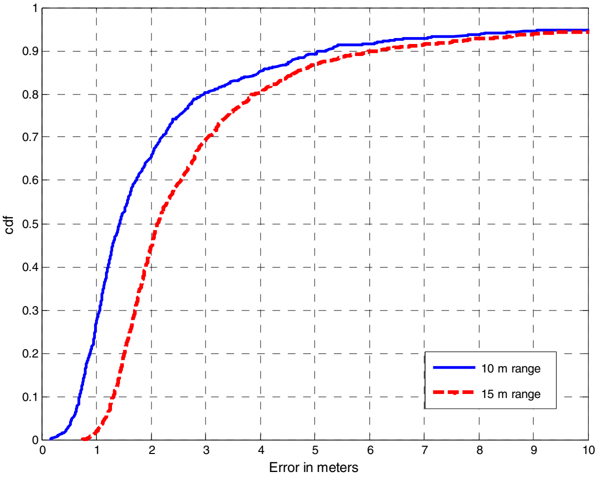


Fig. 6. Error probability

In general, when we set a higher transmission range, the error value (in meters) increases. All these errors contribute to error propagation in subsequent iterations. If the application allows us to use less accurate position estimates, full coverage will be achieved faster. In that case less number of iterations are required; communication overhead is significantly reduced as well as the computation/processing costs. The main goal is to identify the optimum threshold for a certain application and the required accuracy.

5 Conclusion

Cooperative positioning has received broad significant interest, from the robotics, optimization, and wireless communications communities [5]-[13]. While positioning and navigation have a long history, the challenge is to allow nodes which are out of range of any known reference locations to become aware of its location through cooperation, and hereby increase localization performance in terms of both accuracy and coverage. We propose an interactive cooperative positioning framework as a first step towards a distributed solution and able to adapt to a variety of scenarios. This solution provides a way to expand the network coverage in a step-by step fashion by exploiting the localization of known nodes, and future work will address further the application of Utility functions as a means of identifying the most useful nodes to form a member of the cooperative subset for enhancing positioning accuracy.

Acknowledgments. This work has been performed in the framework of the ICT projects ICT-217033 WHERE and ICT-248894 WHERE2 which are partly funded by the European Union.

References

1. ICT-WHERE project (Wireless Hybrid Enhanced Radio Estimators), `http://www.kn-s.dlr.de/where/`
2. Yang, Z., Liu, Y.: Quality of trilateration: Confidence based iterative localization. IEEE Transactions on Parallel and Distributed Systems (May 2009)
3. Gezici, S., Guvenc, I., Sahinoglu, Z.: On the performance of linear least-squares estimation in wireless positioning systems. In: IEEE International Conference on Communications, ICC 2008, Beijing, China, pp. 4203–4208 (2008)
4. Qasem, H., Reindl, L.: Precise wireless indoor localization with trilateration based on microwave backscatter. In: IEEE Annual Wireless and Microwave Technology Conference, WAMICON 2006, Clearwater, FL, USA, pp. 1–5 (2006)
5. Mao, G., Fidan, B., Anderson, B.: Wireless sensor network localization techniques. Computer Networks: The International Journal of Computer and Telecommunication Networking 51(10), 2529–2533 (2007)
6. Shi, Q., Correal, N., Niu, F.: Performance comparison between TOA ranging technologies and RSSI ranging technologies for multi-hop wireless networks. In: IEEE 62nd Vehicular Technology Conference VTC 2005 Fall, Dallas, TX, USA, pp. 434–438 (September 2005)
7. Wu, C., Sheng, W., Zhang, Y.: Mobile self-localization using multi-dimensional scaling in robotic sensor networks. International Journal of Intelligent Control and System 11(3), 163–175 (2006)
8. Costa, J., Patwari, N., Hero, A.: Distributed weighted-multidimensional scaling for node localization in sensor networks. ACM Transactions of Sensor Networks (TOSN) 2(1), 39–64 (2006)
9. Niculescu, D., Nath, B.: Ad hoc positioning system (APS). In: IEEE Global Telecommunications Conference GLOBECOMM 2001, San Antonio, TX, USA, vol. 5, pp. 2926–2931 (November 2001)

10. Savarese, C., Raabey, J.: Robust positioning algorithms for distributed ad-hoc wireless sensor networks. In: USENIX Technical Annual Conference, Monterey, CA, USA, pp. 317–328 (June 2002)
11. Savvides, A., Han, C., Srivastava, M.: Dynamic fine-grained localization in ad-hoc networks of sensors. In: 7th ACM international conference on Mobile computing and networking (Mobicom), Rome, Italy, pp. 166–179 (July 2001)
12. Aslindi, N., Pahlavan, K., Alavi, B., Li, X.: A novel cooperative localization algorithm for indoor sensor networks. In: IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2006, Helsinki, Finland, pp. 1–6 (2006)
13. Langendoen, K., Reijers, N.: Distributed localization in wireless sensor networks: a quantitative comparison. Elsevier Computer Networks: The International Journal of Computer and Telecommunication Networking 43(4), 499–518 (2003)
14. Patwari, N., Ash, J., Kyperountas, S., Hero, A., Moses, R., Correal, N.: Locating the nodes. IEEE Signal Processing Magazine 22(4), 54–69 (2005)

Increasing the VoIP Capacity through MAP Overhead Reduction in the IEEE 802.16 OFDMa Systems

Vitaliy Tykhomyrov

Telecommunication laboratory, University of Jyväskylä, Finland
`vitaliy.tykhomyrov@jyu.fi`

Abstract. One of the main issues with supporting VoIP service over 802.16 networks is the signalling overhead caused by the downlink MAP messages due to frequent transmissions and small packets. To decrease the MAP overhead, the 802.16 standard proposes some mechanisms, such as the compressed MAP and sub-MAPs. In this paper, we show by means of extensive dynamic simulations that sub-MAPs can reduce dramatically the signalling overhead associated with VoIP traffic and significantly improve overall VoIP capacity. At the same time, since sub-MAPs are more sensitive to packet drops, they tend to increase the number of HARQ retransmissions in downlink and transmission delays in the uplink direction.

Keywords: IEEE 802.16, VoIP, Signalling overhead.

1 Introduction

IEEE 802.16 is a standard for wireless broadband access networks [1] that can provide a high-speed wireless access to the Internet for home and business subscribers. It provides the missing link for the *last mile* connection in metropolitan area networks where DSL (Digital Subscriber Line), Cable and other broadband access methods are not available or are too expensive. IEEE 802.16 also offers an alternative to satellite Internet services for rural areas and allows mobility of the customer equipment. The standard is concerned with the air interface between a subscriber station (SS) and a base station (BS).

IEEE 802.16 has been developed before other beyond-3G standards, such as LTE (Long Term Evolution), but there are a few key areas where the performance of 802.16 systems can be improved. Voice over IP (VoIP) service is one of them. One of the key areas for the current revision of 802.16 is the increasing VoIP capacity. The VoIP capacity of any 802.16 OFDMa system is related to the associated overhead. Overhead is important for VoIP applications due to the frequent transmission and small packet size. In the 802.16 system, much of

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 590–603, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

the overhead associated with VoIP traffic occurs in the MAP messages, since dynamic scheduling is used to support VoIP.

To decrease the MAP overhead, the 802.16 standard [2] proposes a few mechanisms, such as the compressed MAP and sub-MAPs. Further enhancements to the 802.16 system [5] introduce persistent allocations.

In this paper we study the sub-MAPs in VoIP applications and analyze how the sub-MAPs can reduce the overhead associated with VoIP traffic and improve overall VoIP capacity.

MAP overhead reduction in VoIP applications has not been studied thoroughly, especially in the IEEE 802.16 networks. In [7], the authors propose a new optimization model and evaluate the performance of a dynamic OFDMa system with inband signalling in terms of how the signalling overhead affects the system performance. However, they consider the signalling overhead only in the downlink direction, even though the signalling overhead of both the downlink and uplink affects the system throughput. In [12], the authors address the problem of allocation representation of VoIP packets and propose an efficient uplink mapping scheme that decreases the size of the allocation map in the IEEE 802.16e OFDMa system. They also present analytical and simulation models to evaluate the performance of the VoIP services. Their results show that the signalling overhead is greatly decreased when the proposed mapping scheme is used. However, the proposed mapping scheme does not conform to the IEEE 802.16 standard since it requires some modifications. Furthermore, their simulator implementation does not contain all the main features of the IEEE 802.16 standard, such as error modeling. In [6], the authors focus on features and solutions used in the IEEE 802.16 standard to support voice traffic and optimization concepts such as persistent allocation. In order to study VoIP performance, they implemented the persistent scheduling scheme in a system-level simulator. The authors state that their simulator complies with the baseline configuration and simulation assumptions in the 802.16m evaluation methodology [3], but they do not provide any description of what is implemented. In [14], the authors consider an AMC scheme for the sub-MAPs to reduce the MAP signaling overhead without explicit information on the channel condition. Indeed, the proposed scheme achieves the same coverage as the broadcast MAP while significantly enhancing the VoIP capacity. However, the authors do not describe their implemented simulation environment, and therefore there is no information whether it does contain all the main features of the IEEE 802.16 standard. Moreover, the authors do not consider the IEEE 802.16m Evaluation Methodology Document [3]. In order to evaluate the MAP overhead, the authors use only 4 MCS levels, while the basic 802.16e system operates 11 different MCS levels.

The rest of this paper is organized as follows. Section 2 provides an insight on VoIP scheduling in the IEEE 802.16. Section 3 presents several simulation scenarios and simulation results. Finally, Section 4 concludes the article and outlines further research directions.

2 VoIP Scheduling and Sub-MAPs in IEEE 802.16

2.1 802.16 Scheduler Implementation

Extended real-time polling service (ertPS) is designed to support real-time service flows that generate variable-size data packets on a periodic basis, such as Voice over IP services with silence suppression. On the downlink, the BS is smart enough to control directly the scheduling of VoIP traffic and allocation of the resources. For the uplink, the BS periodically assigns UL resources according to the requested size, until the SS requests another bandwidth size.

To obtain dynamic simulation results we have implemented our own 802.16 BS scheduler in the NS-2 simulator [11]. The 802.16 BS scheduler accounts for connection parameters, scheduling class type, modulation and coding scheme (MCS), the queue size, and the bandwidth request size. Depending on the direction, the scheduler analyzes either the bandwidth request size sent by the SS or the queue size at the BS.

As for the ertPS class, the 802.16 scheduler allocates N slots for each VoIP connection:

$$N = \begin{cases} 0, & \text{if } R_{size} = 0 \\ \frac{B*G}{S*FPS}, & \text{if } R_{size} > 0, \end{cases} \tag{1}$$

where R_{size} is a bandwidth request size sent by the SS (or the downlink queue size), B is a bandwidth requirement which corresponds to the maximum sustained traffic rate of the VoIP connection QoS profile, S is a slot size as governed by the connection MCS, which determines the number of bytes the SS can send within one slot, FPS represents the number of 802.16 frames per second, and finally G is a grant interval in frames. The latter parameter is usually set to the VoIP codec frame inter-arrival time, e.g., every fourth frame.

There is also a small recovery mechanism that handles lost UL-MAP messages that prevents the SS from transmitting in the uplink. If the uplink request size R_{size} starts grow, the scheduler analyze the uplink request value and temporarily doubles or even triples the size of the UL grant.

More details on the implemented scheduler and support for other scheduling classes are given in [10].

2.2 Sub-MAP Messages

In order to reduce the data bandwidth overhead in sending DL-MAP or UL-MAP, the allocation of data bursts can be achieved by utilizing different types of messages that can be transmitted using more efficient modulation coding schemes (MCSs). The 802.16 standard introduces sub-MAPs that allow for splitting a MAP message into a number of independent messages, each of which is encoded with a more efficient MCS. Sub-MAPs follow the compressed MAP as shown in Fig. 1. The sub-MAP format is quite similar to the compressed MAP with a few additional enhancements, such as the CRC-16 field instead of CRC-32.

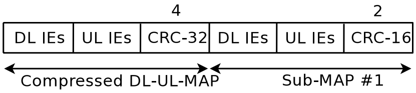


Fig. 1. Compressed MAP with sub-MAP

By using sub-MAPs, data burst allocation information can be transmitted more efficiently. The current version of the 802.16 standard supports up to three sub-MAP messages. To optimize burst allocation efficiency, different algorithms for dividing SSs and choosing an appropriate sub-MAP for data burst allocation can be used. For instance, SSs can be divided into different groups each assigned to a different sub-MAP based on their SINR (Signal to Interference-plus-Noise Ratio). As a result, signalling overhead for sending DL-MAP and UL-MAP is significantly reduced. The only drawback of the sub-MAP message is that if it is dropped, then both the DL-MAP and UL-MAP entries are lost. However, similarly to a compressed MAP message, the sub-MAP should be transmitted with quite a robust MCS to ensure that all the stations receive it correctly. On the other hand, sub-MAPs with a more robust MCS will send less data when compared to other sub-MAPs with a more efficient MCS. Thus, choosing an optimal MCS is a tradeoff between robustness and efficiency.

The 802.16 specification just defines the maximum number of sub-MAPs that can appear in a frame. The exact number, configuration, and MCS to encode a particular sub-MAP are left undefined. We have implemented a simple yet efficient algorithm to build sub-MAPs based on the number of bursts the BS scheduler allocates in a frame. In a few words, it starts a sub-MAP on a particular MCS if that MCS has the biggest number of Information Elements (IEs). Thus, each MCS can be assigned a weight that determines a preference for a sub-MAP message:

$$w_{\text{MCS}} = \frac{\sum S_i^{\text{IE}}}{S^{\text{slot}}}, \tag{2}$$

where S_i^{IE} is the IE size measured in bytes and S^{slot} is the slot size that corresponds to the MCS, for which a weight is calculated. Since the weight determines only a preference for a particular MCS where we might build a sub-MAP, we need an iterative algorithm, a simplified form of which is shown in Fig. 2. The algorithm comprises the following stages:

1. Calculate a weight value for each MCS. Based on the number of uplink and downlink IEs, i.e., the number of data bursts that are encoded with the given MCS, each MCS is assigned a weight value that determines its preference for a sub-MAP candidate. To simplify further manipulations, the list is sorted based on the weight values in the descending order.
2. Consider an MCS as a candidate for a sub-MAP. The algorithm takes the (next) MCS with the highest weight value, adds a sub-MAP, and estimates the total number of slots that a new sub-MAP configuration needs. If it reduces the total signalling overhead, then the MCS is saved into a permanent sub-MAP configuration. Otherwise, the MCS is just skipped. To determine

whether the (next) MCS with the highest weight value reduces the total signalling overhead, the algorithm compares the total number of slots needed to encode IEs with the previous sub-MAP configuration. If the overhead is smaller in terms of slots, then update the permanent sub-MAP configuration.
3. The algorithm works until the maximum number of sub-MAPs is constructed or until all the MCSs are processed.

More details on the sub-MAPs as well as a full description of the implemented algorithm are given in [13].

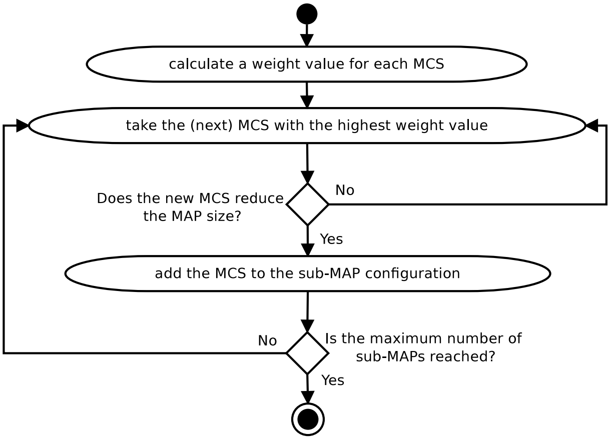

calculate a weight value for each MCS
take the (next) MCS with the highest weight value
Does the new MCS reduce the MAP size?
No
Yes
add the MCS to the sub-MAP configuration
No
Is the maximum number of sub-MAPs reached?
Yes

Fig. 2. Sub-MAP construction algorithm

3 Simulations

This section presents the dynamic simulation results of sub-MAPs with the VoIP application in the 802.16 network. To run simulations, we have implemented the 802.16 MAC and PHY levels in the NS-2 simulator [11]. The MAC implementation contains all the main features of the IEEE 802.16 standard, such as downlink and uplink transmission, connections, MAC PDUs, packing and fragmentation, the contention and ranging periods, the MAC level management messages, and the ARQ mechanism. The HARQ implementation supports Type I, i.e., chase combining (CC) [2].

To speed up simulations, we do not model all the PHY details but rather rely upon the effective SINR trace files taken from the system level simulator, where we modeled 19 cells with 3 sectors per each cell. This provides realistic wireless channel variations, which cause packet errors and drops. The relevant parameters are given in Table 1. All the other PHY mechanisms, such as channel measurements, channel reporting, link adaptation, and scheduling are present and explicitly modeled in the simulation environment.

Fig. 3 shows the network structure we used in the simulations. We concentrate on a single 802.16 sector with the BS and a number of SSs. The 802.16 network

Table 1. System level parameters

Parameter	Value
Reuse factor	1/3
Inter-site distance	1.5 km
Path loss model	UMTS 30.30
Slow fading std.	8 dB
Fast fading	Ped B (60%), Veh A (40%)
Antenna technique	SISO (1x1)
Antenna pattern BS/MS	3GPP / Omnidirectional
Antenna height BS/MS	32 / 1.5 m
Tx power BS/MS	20 / 0.2 W

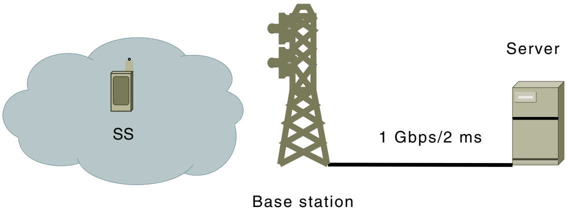


Fig. 3. Network structure

parameters are presented in Table 2[1]. Even though we study a symmetrical VoIP service, we choose the TDD DL/UL ratio in such a way that more resources are allocated to the DL sub-frame where signalling messages reside. While modeling the DL signaling messages, such as MAPs and sub-MAPs, we account for the fact that they can be dropped and apply the same error model as we do for normal data PDUs. As a result, if an SS looses a MAP or a sub-MAP message, it cannot receive or transmit data. It allows us to study how sub-MAPs impact performance of the VoIP service.

The BS runs the throughput-fair scheduling algorithm, general description of which is presented in [10]. In section 2.1, we gave a more detailed description of the VoIP scheduler. The link adaptation mechanism ensures the target FEC BLER of 10^{-1} for the HARQ-enabled connections.

Each SS establishes a basic management connection to exchange management messages with the BS. In addition, each SS has a bi-directional VoIP transmission with the server carried over two ertPS connections. The VoIP application parameters given in Table 3 are taken from the IEEE 802.16m Evaluation Methodology Document [3]. However, to stress the system, we model the worst case scenario, where each VoIP SS has the constant active bi-directional VoIP transmission during each simulation run. In addition, we limit the VoIP connection queue length to 3 SDUs to meet the air interface transmission delay of less than 100 ms. The ertPS connections use HARQ as a retransmission mechanism because ARQ cannot always ensure required delay limits. Furthermore, we turn the HARQ PDU

---

[1] These parameters conform to the WiMAX Forum mobile system profile [4].

Table 2. 802.16 network parameters

Parameter	**Value**
PHY	OFDMa
Bandwidth	10 MHz
Duplexing mode	TDD
Frames per second	200
Cyclic prefix length	1/8
TTG+RTG	296+168 PS
OFDM symbols	48
DL/UL symbols	28/19
DL/UL subcarrier alloc.	DL PUSC/UL PUSC
DL/UL slots	420/210
Channel report type / interval	CQICH / 20ms
Channel measurements DL/UL	preamble / data burst
Channel measurements filter	EWMA , $\alpha = 0.25$
Compressed MAPs	ON
sub-MAPs / max. number	ON / 3
Ranging transm. opport.	2
Ranging backoff start/end	1/15
Request transm. opport.	4
Request backoff start/end	2/15
CDMA codes	256
ranging+periodic ranging	64
bandwidth request	192
handover	–
HARQ	Type I (CC)
HARQ channels	16
HARQ buffer size	2048 B (per channel)
HARQ shared buffer	ON
HARQ max. retransmissions	4
HARQ ACK delay	1 frame
HARQ PDU SN	OFF
Fragmentation/packing	OFF

sequence numbering off to cater for smaller delays[2]. In addition, we disable both packing and fragmentation for VoIP, which in conjunction with a proper VoIP scheduler ensures absence of unnecessary MAC level overhead. Uplink ertPS connections use the CDMA contention as the resumption mechanism to inform the BS that there is an uplink data to be transmitted. As simulated in [9], this is a more efficient way when compared to polling.

Extensive simulations were conducted to study VoIP capacity of the whole system. For these purposes, we varied the number of VoIP connections in the system. A different approach is to inject a large number of VoIP connections and then let the admission control module to drop connections if the network capacity is exceeded [8]. Since we do not aim at studying the admission control module, we just disabled it.

For each simulation case, we made 32 simulation runs to obtain proper confidence intervals. Each simulation run lasted for 13 seconds, where the actual

---

[2] The HARQ PDU ordering is usually turned on for the TCP connections where the TCP receiver may react unpredictably for packets arriving in the wrong order. In case of VoIP, a receiver usually implements a so-called de-jitter buffer, depth of which varies from 20 ms to 60 ms. An alternative VoIP configuration is to enable PDU SN and tune the HARQ ordering buffer timeout based on the maximum number of HARQ retransmissions.

Table 3. VoIP parameters

Parameter	Value	
Codec	G.729	
Active state	100%	
Aggregation interval	20 ms	
Voice Payload	20 bytes	
802.16 Generic MAC header HARQ CRC	6 bytes 2 bytes	
IP/UDP/RTP headers	40 bytes (no PHS)	2 bytes (PHS)
Total VoIP packet size	68 Bytes	30 Bytes

data transmission starts at the 3rd second because the first SSs have to enter the cell and register at the BS.

3.1 Performance Criteria

In this sub-section we describe two main VoIP performance criteria that we used: delays and packet loss ratio.

Delays. The VoIP SDU delay is defined as

$$Delay = T^{dep} - T^{arr}, \tag{3}$$

assuming that the packet destined for SS arrives at the BS(SS) at time T^{arr} and is delivered to the SS(BS) at time T^{dep}.

Following [3], we check that 98% of connections deliver 98% of VoIP packets within the delay bound of 100 ms. For these purposes, first for each connection we determine percentage of packets that meet the delay bound of 100 ms. Then, these values are used to build another CDF (cumulative distribution function) that shows how many connections meet the target requirements.

Packet Loss Ratio. According to [3], the packet loss ratio per connection is defined with the following criterion:

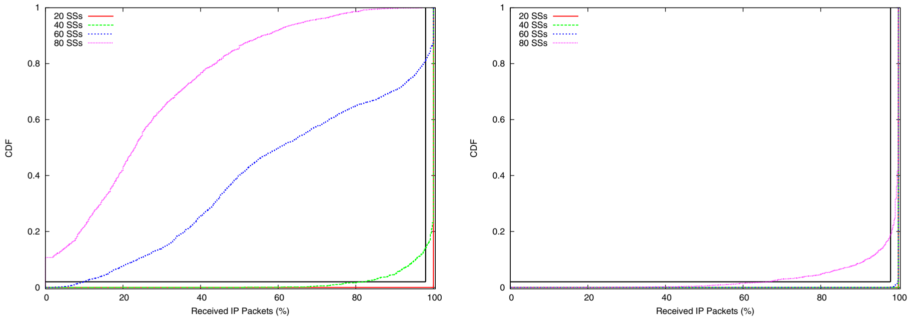
$$R^{loss} = 1 - \frac{P^{delivered}}{P^{total}}, \tag{4}$$

where $P^{delivered}$ includes the total number of successfully delivered packets and P^{total} includes packets that were transmitted over the air interface and packets that were dropped prior to transmission. If more than 2% of the VoIP packets are dropped, erased or not delivered successfully to the SS within the delay bound of 100 ms, then SS is not satisfied.

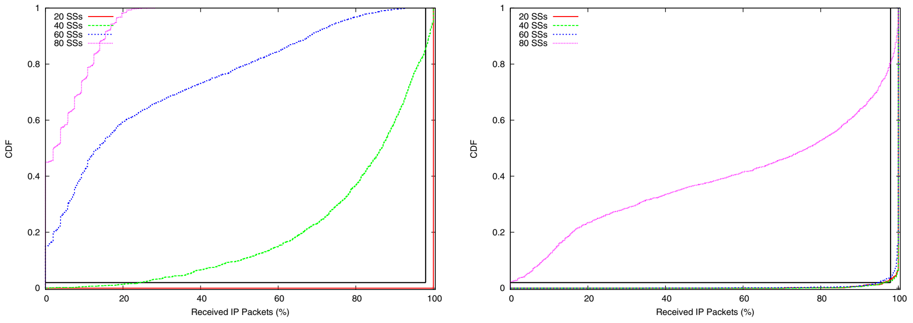
In modeling traffic from delay sensitive applications, packets may be dropped if packet transmissions are not completed within a specified delay bound. The impact of such dropped packets can be captured in the packet loss rate.

3.2 Delays

In this sub-section we analyze how injecting a different number of VoIP connections and enabling sub-MAPs impact the VoIP capacity and associated transmission delays. To see the cases when SSs do not meet their delay requirements, we introduce boundary lines for X and Y - axis that show whether 98% of packets are delivered successfully to the 98% SSs within the delay bound of 100 ms. We consider separately a case with disabled sub-MAPs and enabled sub-MAPs.



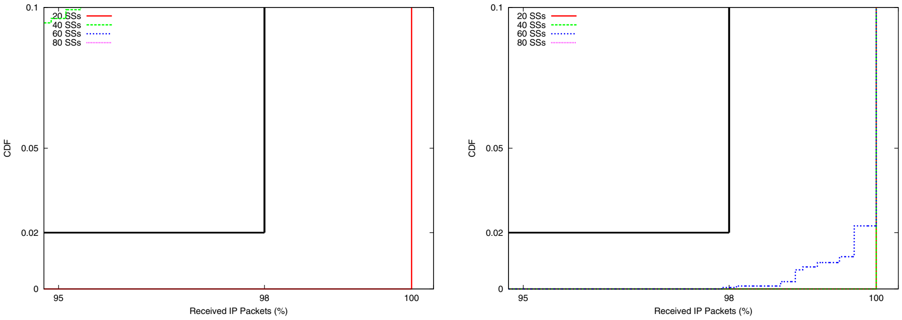
(a) disabled sub-MAPs, DL (b) enabled sub-MAPs, DL



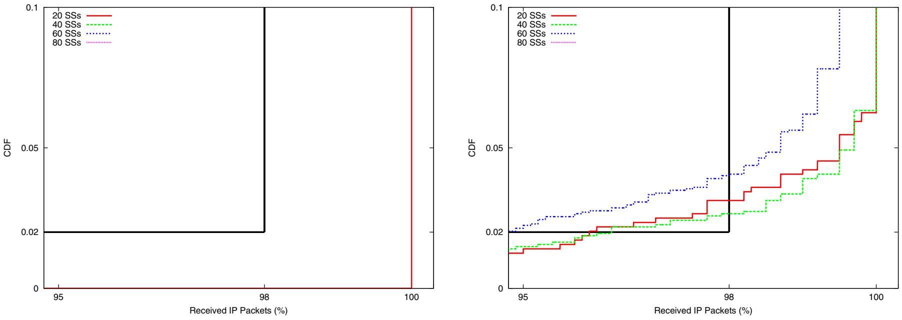
(c) disabled sub-MAPs, UL (d) enabled sub-MAPs, UL

Fig. 4. VoIP SDU E2E delay CDF

Results with end-to-end delay CDFs are presented in Fig. 4(a) and Fig. 4(c) for the downlink and uplink directions respectively. Fig. 5(a) and Fig. 5(c) demonstrate the same case with more detailed elaboration for the downlink and uplink parts respectively. Fig. 4(a) shows that if sub-MAPs are disabled then the downlink VoIP capacity is only 20 SSs, whereas a bigger number of SSs start to experience downlink delays larger than 100 ms. As can be seen from Fig. 4(c), the uplink capacity is also limited by 20 SSs.



(a) disabled sub-MAPs, DL (b) enabled sub-MAPs, DL



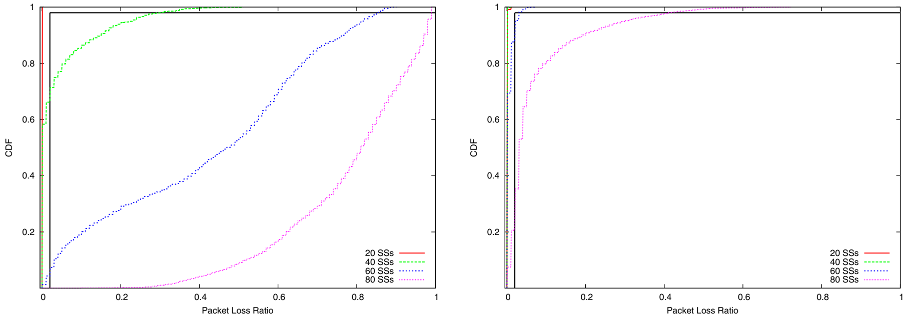
(c) disabled sub-MAPs, UL (d) enabled sub-MAPs, UL

Fig. 5. VoIP SDU E2E delay CDF

Next, we enable sub-MAPs and analyze the upper limits for the VoIP capacity. The results are shown in Fig. 4(b) and Fig. 4(d) for the downlink and uplink directions. When compared to Fig. 4(a), where the VoIP capacity is limited by 20 SSs in the downlink direction, Fig. 4(b) illustrates clearly that enabled sub-MAPs improve overall VoIP capacity up to 60 VoIP connections. In the uplink, as can be seen in Fig. 4(d), the VoIP capacity is around 60 SSs.

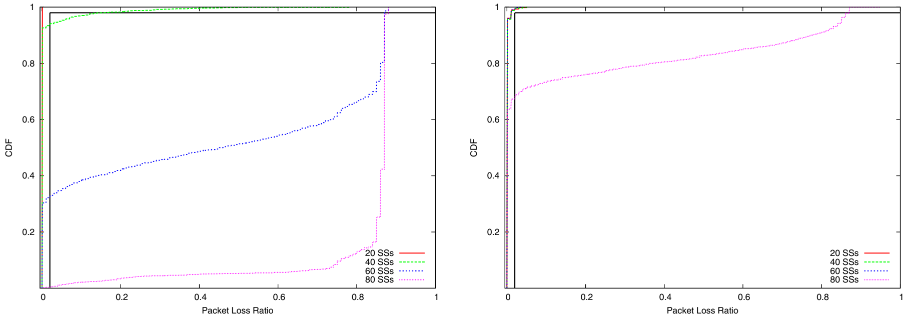
Fig. 5(b) and Fig. 5(d) show more detailed elaboration for the downlink and uplink parts respectively. Having compared Fig. 5(a) and Fig. 5(b), it is noticeable that enabled sub-MAPs start to bring more gain.

Fig. 5(d) also presents eloquently how enabled sub-MAPs tend to increase transmissions delays for a small number VoIP connections. When compared to Fig. 5(c), even 20 VoIP connections have slightly larger delays. The reason for this phenomena is dropped sub-MAP messages. If it is dropped, then both the DL-MAP and UL-MAP entries are lost. If an SS fails to receive the sub-MAP message, it cannot transmit anything in the UL direction thus causing queue growths. It takes some time for the BS scheduler to detect this situation and allocate a larger UL grant.



(a) disabled sub-MAPs, DL

(b) enabled sub-MAPs, DL



(c) disabled sub-MAPs, UL

(d) enabled sub-MAPs, UL

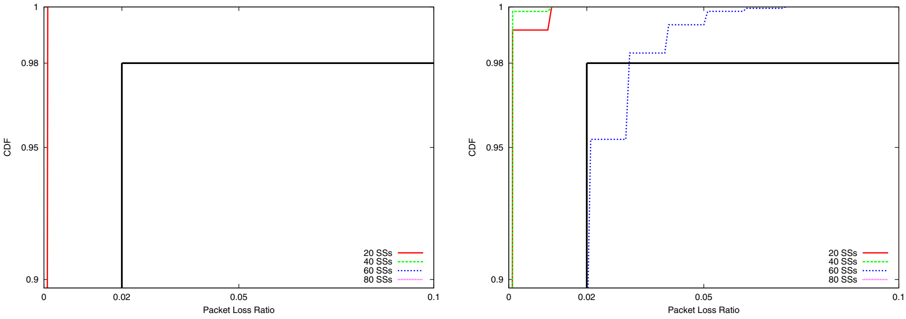
Fig. 6. VoIP Packet Loss Ratio

3.3 Packet Loss Ratio

In this sub-section we analyze how different numbers of VoIP connections and sub-MAPs affect the VoIP capacity and the packet loss ratio. As in the case of delay analysis, we also apply boundary lines for X and Y - axis to ensure that 98% of SSs experience packet drops of less than 2%.

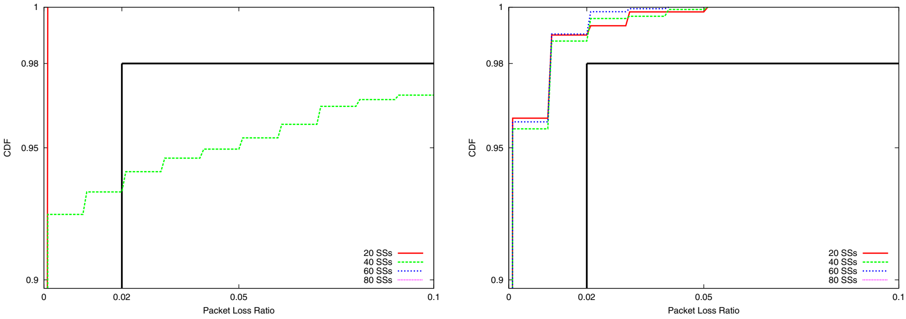
The results for packet loss ratio CDFs with disabled sub-MAPs are presented in Fig. 6(a) and Fig. 6(c) for the downlink and uplink parts, while Fig. 7(a) and Fig. 7(c) demonstrate more detailed elaboration for the downlink and uplink parts respectively. As seen from Fig. 6(a) and Fig. 6(c), the only case with 20 SSs shows the packet loss ratio of less than 2% of both the downlink and uplink directions, while all the other cases exceed the target packet loss ratio due to frequent packet drops caused by queue overflows.

As we enable sub-MAPs, we can decrease drastically VoIP packet drops because now the system has more resources to serve VoIP connections. As can be seen from Fig. 6(b) and Fig. 7(b), almost 60 DL VoIP connections can be served. As for the uplink, as can be seen from Fig. 6(d) and Fig. 7(d), enabled sub-MAPs



(a) disabled sub-MAPs, DL

(b) enabled sub-MAPs, DL



(c) disabled sub-MAPs, UL

(d) enabled sub-MAPs, UL

Fig. 7. VoIP Packet Loss Ratio

decrease the packet loss ratio up to 60 SSs, but cannot meet the defined 2% with 80 SSs.

4 Conclusions

This paper contributes to evaluating the VoIP capacity with enabled sub-MAPs in the IEEE 802.16 OFDMa system. We ran complex dynamic simulations with all the major radio resource management algorithms of the IEEE 802.16 system and the VoIP service. The results demonstrate that it is reasonable to enable sub-MAPs to support more VoIP connections. Otherwise, the signalling overhead, as a part of the 802.16 air interface, creates a bottleneck for the 802.16 OFDMa system. In particular, our simulation results show the significant VoIP capacity improvement. However, the obtained performance with enabled sub-MAPs may vary depending on the network parameters and traffic load.

It is worth mentioning that sub-MAPs must be transmitted with quite a robust MCS to ensure that all the SSs receive them correctly. Otherwise, a loss of the downlink sub-MAP results in a situation when the BS reschedules the same data because an SS does not send a positive HARQ ACK message. In the uplink direction, if an SS cannot decode a sub-MAP then it fails to transmit any data. As a result, uplink queues start to grow thus increasing the transmission delays. As a possible solution, uplink sub-MAP messages may be encoded with a more robust MCS when compared to the downlink direction.

An interesting outcome of these dynamic simulations is that sub-MAPs have a negative impact on the UL channel estimation. If the sub-MAP encoding an UL allocation is lost, then an SS does not transmit thus preventing the BS from estimating the UL channel state that varies due to the fast fading and SS movements. A possible solution is a so-called UL sounding defined in the 802.16 specification.

Our further research will aim at studying how sub-MAP messages can be used in conjunction with persistent allocations. It is anticipated that even more VoIP connections can be admitted. On the other hand, a static nature of persistent allocations and a higher error rate of sub-MAPs may cause performance degradation of the VoIP service.

Acknowledgments

We express our acknowledgments to Alexander Sayenko (Nokia Siemens Networks) and Olli Alanen (Magister Solutions) who provided valuable comments on the simulation setup and results. We also would like to thank Henrik Martikainen, Oleksandr Puchko and Vesa Hytönen (University of Jyväskylä / Telecommunication laboratory) for their contribution to the implementation of the 802.16 MAC and PHY levels in the NS-2 simulator. Special thanks to Timo Hämäläinen (University of Jyväskylä / Telecommunication laboratory) for supervising this work.

References

1. Air interface for fixed broadband wireless access systems. IEEE Standard 802.16 (June 2004)
2. 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. IEEE Standard 802.16e (December 2005)
3. IEEE 802.16m evaluation methodology document (EMD). IEEE 802.16 Broadband Wireless Access Group. (March 2008)
4. WiMAX Forum Mobile System Profile, Release 1.0 Approved Specification, Revision 1.6.1 (April 2008)
5. Air interface for broadband wireless access systems. IEEE Standard 802.16 (Rev. 2) (May 2009)
6. Fong, M.-h., Novak, R., Mcbeath, S., Srinivasan, R.: Improved VoIP capacity in mobile WiMAX systems using persistent resource allocation. IEEE Communications Magazine 46(10), 50–57 (2008)
7. Gross, J., Geerdes, H.-F., Karl, H., Wolisz, A.: Performance analysis of dynamic OFDMA systems with inband signaling. IEEE Journal on Selected Areas in Communications 24(3), 427–436 (2006)

8. Lakkakorpi, J., Sayenko, A.: Measurement-based connection admission control methods for real-time services in IEEE 802.16e. In: Second International Conference on Communication Theory, Reliability, and Quality of Service, CTRQ 2009, pp. 37–41 (July 2009)
9. Lakkakorpi, J., Sayenko, A.: Uplink VoIP delays in IEEE 802.16e using different ertPS resumption mechanisms. In: Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pp. 157–162 (October 2009)
10. Sayenko, A., Alanen, O., Hämäläinen, T.: Scheduling solution for the IEEE 802.16 base station. Computer Networks 52, 96–115 (2008)
11. Sayenko, A., Alanen, O., Martikainen, H., Tykhomyrov, V., Puchko, O., Hämäläinen, T.: WINSE: WiMAX NS-2 Extension. In: 2nd International Conference on Simulations Tools and Techniques (March 2009)
12. So, J.-W., Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do: An efficient uplink mapping scheme for VoIP services in the IEEE 802.16e OFDMA system. AEU - International Journal of Electronics and Communications 62, 768–776 (2008)
13. Tykhomyrov, V., Sayenko, A., Puchko, O., Hämäläinen, T.: Decreasing the MAP overhead in the IEEE 802.16 OFDMA system. In: European Wireless Conference (2010) (accepted for publication)
14. Yeom, J.-H., Lee, Y.-H.: Efficient transmission of multicast maps in IEEE 802.16e. IEICE Transactions 91-B(10), 3157–3161 (2008)

Multi-radio Cooperative ARQ in Wireless Cellular Networks: A MAC Layer Perspective

J. Alonso-Zárate[1], E. Kartsakli[2], L. Alonso[2], M. Katz[3], and Ch. Verikoukis[1]

[1] Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)
Av. Carl Friedrich Gauss 7, CTTC, 08860 Castelldefels, Barcelona, Spain
{jesus.alonso,cveri}@cttc.es
[2] Department of Signal Theory and Communications,
Universitat Politècnica de Catalunya (UPC)
Av. Esteve Terradas, 7, EPSC, Campus UPC, 08860 Castelldefels, Barcelona, Spain
{ellik,luisg}@tsc.upc.edu
[3] University of Oulu, Finland
marcos.katz@ee.oulu.fi

Abstract. Multi-Radio Cooperative Automatic Retransmission Request (MC-ARQ) schemes are introduced in this paper within the context of hybrid networks which combine long-range and short-range communications. Since the number of wireless devices is incessantly increasing, it is frequently possible to establish a spontaneous cooperative cluster in the close proximity of any wireless device. These devices forming the cluster are connected to both a cellular-based network such as WiMAX, 3G, or LTE and a short-range network based on technologies such as WLAN, Zigbee, Bluetooh, or UWB, among other possibilities. The main idea behind the proposed MC-ARQ scheme is that, upon transmission error through the cellular interface, retransmission can be requested to the wireless grid surrounding the destination device using the short-range interface instead of the primary cellular link. Therefore, besides the cooperative diversity attained with C-ARQ schemes, the traffic load in the cellular interface is reduced benefiting thus a high number of users and reducing both energy consumption and interference. The Persistent Relay Carrier Sensing Medium Access (PRCSMA) protocol is presented as an example of solution for the MAC layer in this emerging new topic.

Keywords: cooperative communications, heterogeneous networks, cooperative ARQ, Medium Access Control (MAC).

1 Introduction

Although the concept of cooperation in wireless communication networks was first presented almost four decades ago [1], the seminal works of Sendonaris et al. [2] and Laneman [3] triggered a vast amount of research in the topic since 2000. Cooperative communications is still today a very popular and highly diversified research topic [4]. Most of the research efforts so far have been focused on fundamental and theoretical studies, while less work has been devoted to developing concrete practical applications of cooperation. Most of the early work on cooperative communications has focused on improving transmission parameters at the physical layer. However, the truly emergence of cooperative communications needs to be supported by extensive research on higher

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 604–617, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

layers of the protocol stack as well as the development of novel business models. We deal in this paper with a simple and practical way of applying cooperation in the real world; wireless grids [5]. A wireless grid is a cooperative spontaneous cluster made of heterogeneous wireless devices in close proximity of each other. These devices are connected to a conventional infrastructure-based cellular network, e.g., to an Access Point (AP) or a Base Station (BS), and they are also connected to each other through short-range links. GSM/GPRS, 3G, LTE, WiMAX or satellite are representative examples of wide area cellular access, while short-range connectivity can be provided by technologies such as Wireless Local Area Network (WLAN), Zigbee, Bluetooth, or UWB among other possibilities. Therefore, a hybrid communication architecture combining centralized and distributed access topologies is considered. Such composite communication architecture, a widely unexplored research field, can benefit the whole value chain, from network, service and content providers, to manufactures as well as the end-users. One of the keys for the success of the wireless grid concept is to develop cooperative strategies for which all interacting devices (or users behind them) will get some advantage, resulting in a natural incentive for users to cooperate.

According to visions of the Wireless World Research Forum (WWRF), by the year 2017, seven trillion wireless devices will be serving seven billion people. Clearly, most of these devices will combine both cellular and short-range communication interfaces. One of the main consequences of these figures is that there will be always a potential cooperative cluster surrounding any wireless device regardless of its specific location. In fact, this is a reasonable assumption even today. It is possible to interconnect a laptop, a mobile phone, and a PDA to create a Personal Area Network (PAN), having thus an already deployed personal wireless grid. This can be extended to office and home environments, where the number of wireless devices is increasing day by day. Although more complex to manage, the wide urban environment could also provide wireless grid availability. This classification is illustrated in Figure 1.

It is worth emphasizing that the wireless grid concept can be in principle implemented with existing technologies, as many commercial wireless devices today integrate onboard multiple air interfaces. In fact, this trend is expected to continue and strengthen in the future. However, so far, a given interface is typically used for a particular application. The concept of wireless grids exploits interoperation of these technologies, as illustrated in Figure 2.

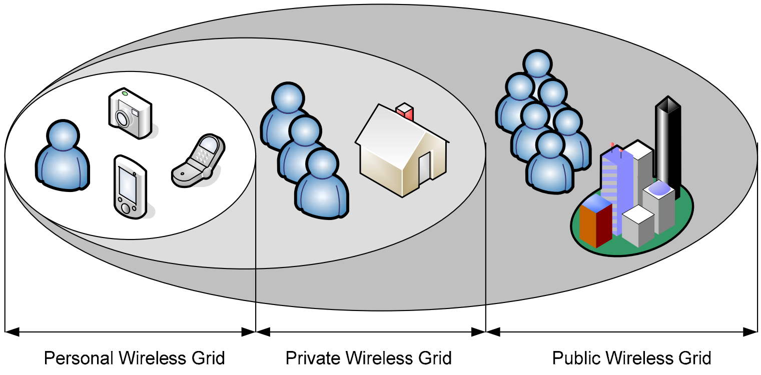


Fig. 1. Different operating scenarios for wireless grids

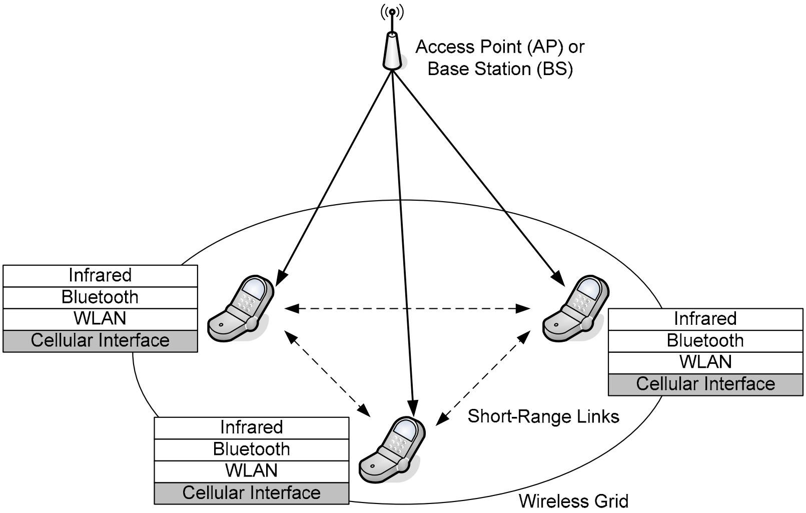


Fig. 2. Wireless Grid: composite network with infrastructure-based networks and peer-to-peer communications

It is worth emphasizing that this concept is different from that of vertical handover, which represents the change of radio interface for seamless communications. In our case, we deal with the interoperation of the different interfaces simultaneously. Note that wireless grids can help in distributing information from the cellular (infrastructure-based) network to the customers in order to improve energy efficiency of wireless devices, to increase network throughput, to increase delivery reliability or to reduce interference to other systems. However, in order to bring cooperation in wireless grids to life, it is still necessary to study and analyze their operation from a wide range of points of view. In fact, the wireless grid concept opens an enormous vast of communication opportunities that can be exploited in several ways.

We present in this paper the concept of the Multi-Radio Cooperative Automatic Retransmission Request (MC-ARQ) scheme at the Data Link Layer (DLC) of wireless grid systems. The main idea is to execute a Cooperative ARQ (C-ARQ) scheme while exploiting the multi-radio capabilities of wireless grids. Since the first contribution of Zimmermann et al. related to C-ARQ in wireless networks [6], a variety of C-ARQ schemes have been proposed as a solution to combat the wireless channel fading and improve the performance of traditional (non-cooperative) ARQ schemes in wireless networks. We will review the main contributions later in Section 0. C-ARQ schemes exploit the broadcast nature of the wireless channel by which a transmission can be heard not only by the intended destination but also by any device in the transmission range of the transmitter. What has been traditionally considered as interference, is used in C-ARQ schemes to provide alternative uncorrelated retransmission paths upon error occurrence, i.e., spatial diversity. The devices which overheard the original transmission can act as spontaneous helpers, partners, or relays and retransmit a copy of the original packet. This avoids a (probably costly in terms of radio resources) retransmission from the source through the same channel where the error has occurred, which might remain in bad conditions for some time due to the space-time correlation of the wireless channel. The MC-ARQ scheme presented in this paper extends this idea to wireless grids with multiple radio interfaces available at each device. Upon the reception of a data packet with errors within the cellular interface, retransmissions can be requested to any of the potential local helpers, i.e., any of the users forming the wireless grids. However, unlike in C-ARQ schemes, these retransmissions can be performed through a different interface, i.e., any of the short-range wireless interfaces available both at destination and at the helpers. Therefore, the MC-ARQ scheme attains:

1. The cooperative diversity gains of C-ARQ schemes as the helpers provide independent transmission paths.
2. The implicit benefits of using short-range communications, i.e., lower transmission power and thus lower energy consumption and interference.
3. The unloading of the cellular link. This is probably the most important achievement since yields a benefit for the whole network and thus can be perceived by the helpers as an incentive to cooperate.

In this paper we analyze the unique characteristics of MC-ARQ schemes from the MAC layer point of view and identify future challenges to be investigated. It should be taken into account that getting a number of devices involved in the communication process requires coordination, which is not costless. We also present the Persistent Relay Carrier Sensing Multiple Access (PRCSMA) protocol, previously described and analyzed in [7] and [8] for plain C-ARQ, as an example of MAC protocol suitable for the execution of the MC-ARQ. It considers that devices in the wireless grid (short-range) can get connected through a CSMA-based interface, such as WLAN 802.11 [9] or Wireless Sensor Networks 802.15.4 [10] based systems. A case study is briefly introduced in this paper to show the improved performance that can be attained in a composite cellular/WLAN network.

The remainder of the paper is organized as follows. In Section 0 we describe the proposed MC-ARQ scheme in the context of wireless grids. In Section 0 we discuss the unique challenges that such schemes pose to the design of the MAC layer. In Section 0 we review the state of the art in the design of cooperative MAC protocols and in Section 0 we identify the PRCSMA as an IEEE 802.11-based MAC protocol suitable for the execution of a MC-ARQ scheme. Some simulation results are discussed in Section 0 and, finally, Section 0 concludes the paper and gives some final remarks.

2 Multi-Radio Cooperative ARQ (MC-ARQ) in Wireless Grids

We consider an infrastructure-based wireless network with a number of wireless devices associated to the cellular-based AP or BS. The terminals are equipped with additional wireless short-range interfaces that enable peer-to-peer communications. Due to the dynamic conditions of the wireless channel within the cellular interface some packets may be received at the destination with unrecoverable errors. These transmission errors can be detected at destination by attaching, for example, a Cyclic Redundancy Code (CRC) to the header of data packets. Due to the broadcast nature of the wireless channel, these transmissions can be overheard by the devices forming the wireless grid around the destination device, likely through independent and uncorrelated transmission paths. Therefore, upon the occurrence of a transmission error, retransmission can be requested either from the source through the cellular interface or, locally from one or more devices in the wireless grid. In the latter case, spatial diversity gains can be attained. The basic concept of cooperative diversity is illustrated in Figure 3. The proposed cooperative scheme can benefit both the involved nodes and the whole network in several aspects. In the case that retransmission is requested at the local level, the signal to interference ratio between neighbor cells is reduced with a consequence to the overall capacity of the network. Moreover, the available bandwidth of the cellular network can be used for another transmission and the total throughput of the cellular network may be increased (as it is freed from retransmitted traffic). In addition, the local short-range retransmission can be done at higher transmission rates and with lower energy consumption profiles. Therefore, the key of the MC-ARQ scheme is to exploit this spatial diversity and to span it to the frequency and technology domains by executing retransmissions through different wireless interfaces.

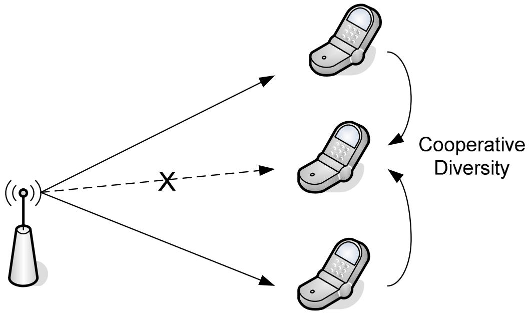


Fig. 3. Cooperative Diversity

The MC-ARQ works as follows: all the devices listen to every ongoing transmission in the cellular interface in order to be ready to cooperate when required. In addition, they keep a copy of any transmitted data packet from the AP or BS (regardless of its destination address) until it is acknowledged by its intended destination. The copy retained by the devices might be stored at each device data buffer or in a different dedicated queue. Scheduling tasks are out of the scope of this paper, but they should be revisited to match the MC-ARQ operation. Whenever a destination receives a data packet with unrecoverable errors through the cellular interface, it broadcasts a retransmission request in the form of a control packet through a short-range wireless interface. A c*ooperation phase* is then initiated. The control packet is referred to as the Call for Cooperation (CFC) packet. A set of the devices within the neighborhood of the destination which overheard the original transmission from the source and receives the CFC from the destination become active helpers and form the concept of wireless grid. Each of these active helpers attempts to retransmit a copy of the original packet to assist in the failed communication. Therefore, the requested retransmissions take place using a short-range technology and thus the main cellular link is unloaded. Although these retransmissions could be performed orthogonally in either time

(TDMA), frequency (OFDMA), or code (CDMA), we focus hereafter on time-orthogonal retransmissions, which might be the simplest approach to implement. Eventually, the destination station might either receive an errorless copy of the original data packet or be able to properly combine the different retransmissions from the helpers to successfully decode the original packet. This event indicates the end of the *cooperation phase* and is notified to the wireless grid through the broadcast of an ACK packet.

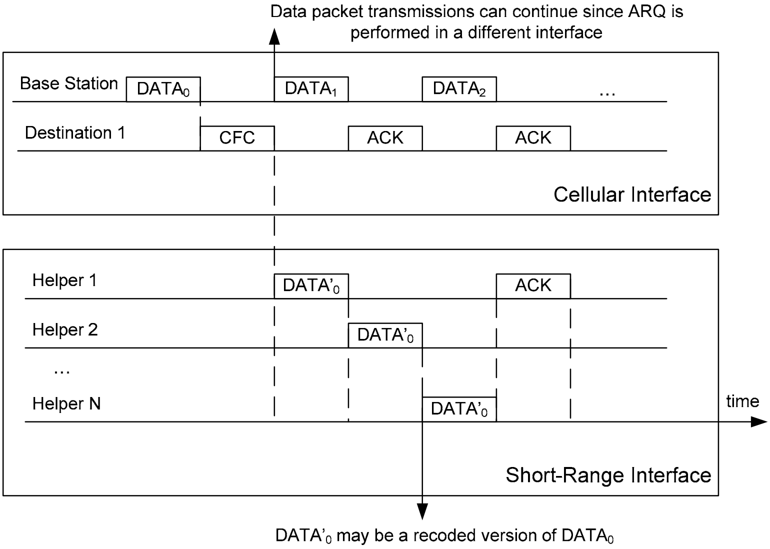


Fig. 4. Multi-Radio Cooperative ARQ scheme

The ideal operation of the MC-ARQ scheme is exemplified in Figure 4 where the communication between a BS and a destination device is assisted by an arbitrary number of helpers. As shown in the picture, the most remarkable benefit derived from the execution of the MC-ARQ scheme is that data packet transmissions in the cellular interface can continue despite the occasional occurrence of transmissions errors. Recall that the MC-ARQ scheme is executed in a different and independent short-range wireless interface, and thus the occupation of the cellular interface for retransmissions is reduced.

The performance of this kind of MC-ARQ schemes is strongly influenced by the following factors:

1. **The helper selection criteria:** The CFC transmitted by the destination may attach some helper selection criteria. For example, it could attach a minimum required Signal to Noise Ratio (SNR) threshold in the reception of either the original data packet or the CFC packet in order to become an active helper. Although the helper selection problem is a very interesting topic itself, it is out of the scope of this paper.

2. **The PHY forwarding technique executed by the active helpers:** according to the specific strategy applied by the helpers it is possible to classify cooperative (helper) techniques as:
    a. *Amplify and forward* techniques, when the helpers transmit an amplified version of the original signal.
    b. *Compress and forward* techniques, when the helpers send a compressed version of the original transmitted signal.
    c. *Decode and forward* techniques, when the helpers transmit recoded copies of the original message. It has to be noted that using decode and forward, the recoding process can be done on the basis of repeating the original codification, recoding the original data (or only a relevant part of it), or using more sophisticated space-time codification 4.
3. **The number of required retransmissions to decode a packet**. This value depends on:
    a. The peer-to-peer channel gains between all the players in the communication, i.e., the source, the destination, and the helpers.
    b. The forwarding technique exploited by the helpers.
    c. The technique exploited by the destination device to combine the different retransmissions received from uncorrelated paths.
4. **The MAC protocol** used for the contention among the different helpers.

In the next section, we describe the specific challenges that an MC-ARQ scheme poses to the MAC sub-layer.

3 MC-ARQ: Challenges at the MAC Layer

The MC-ARQ scheme presented in this paper has some particularities that claim for a redesign of the traditional concept of MAC protocols. This transformation has to be done at three different levels; one at the cellular interface, one at the short-range network formed for the cooperation phase, and another one at the inter-technology ARQ scheme.

First, the MAC protocol executed in the cellular network should enable the overhearing of data transmissions. Typically, in cellular systems each user has some allocated resource, e.g., time slot, frequency band, coding sequence, etc. Therefore, it is necessary to redesign and rethink the access methods of these wide range networks so that at least some users can listen to all other transmissions thus enabling cooperation.

Second, MAC protocols for wireless networks have been traditionally designed on the basis of not only maximizing throughput and minimizing delay, but also achieving fairness among the contending users. In addition, MAC protocols are designed to attain maximum performance in stable conditions, without paying much attention at transitory effects of network start-up. However, in the considered MC-ARQ scheme, upon the initialization of the cooperation phase, the short-range network has the two following unique characteristics:

1. The local sub-network formed by the active helpers surrounding the node claiming for cooperation, i.e., the wireless grid, is *suddenly* set into saturation conditions whenever the cooperation phase is initiated. Upon the transmission of a CFC packet, all the active helpers have a data packet ready to transmit in order

to assist the failed transmission. Therefore, the short-range wireless grid operates in saturation conditions.

2. Fairness might not be a major issue. The main goal is to attempt to assist the failed transmission as fast as possible, minimizing the use of the radio resources for a single transmission.

These two characteristics determine the way MAC protocols should operate within the context of MC-ARQ schemes in wireless grids.

Finally, the redesign of MAC protocols goes beyond the contention among the different helpers in the short-range network and the overhearing at the cellular link. The integration of two different technologies should be accompanied by a joint design of the MAC protocol at both the cellular network and the short-range network. This is a completely unexplored research field. Just as a simple example, the cellular network should positively acknowledge data packets even when they have not been successfully decoded. This may have implications at higher layers of the protocol stack in the light of consistency of the transmitted data.

In order to exemplify how these peculiarities affect the MAC layer design, we present in this paper the PRCSMA protocol as a MAC protocol suitable for the wireless grid part, i.e., the short-range network. The protocol operation is based on the IEEE 802.11 MAC protocol [9], but with some modifications that are required for the sake of backward compatibility and to match the requirements of the MC-ARQ scheme. Similar modifications may be done in the MAC protocol of the 802.15.4 standard [10] in order to operate under the proposed scheme. Before presenting the operation of the protocol in Section 0, in Section 0 we review the state of the art in the design of MAC protocols for cooperative communications, putting the emphasis on the reasons why they are not suitable for the MC-ARQ scheme.

4 Related Work

Several cooperative MAC protocols have been recently proposed, see [11]-[17]. However, these are not designed to support the considered MC-ARQ scheme. In particular, in [11] two versions of the CoopMAC protocol are designed in the context of 802.11b WLANs in order to solve the performance anomaly problem induced by the multi-rate capability of the Distributed Coordination Function (DCF) of the Standard [7]. Korakis et al. implemented the protocol in off-the-shelf WLAN interfaces using open source wireless drivers, as reported in [12]. The main contribution in [12] is the description of the overall implementation process and the limitations found when attempting to implement the protocol. These limitations are mainly due to the constraints imposed by the time sensitive tasks performed by wireless cards' firmware. In addition, the CoopMAC was adapted to wireless networks using directional antennas in [13]. On the other hand, both the Cooperative-MAC (CMAC) and Forward Error Correction CMAC (FCMAC) protocols were presented in [14] within the context of 802.11e networks to improve the performance and to ensure a certain Quality of Service. In [15], the Cooperative Diversity Medium Access with Collision Avoidance (CD-MACA) protocol is proposed within the context of wireless ad hoc networks operating over the CSMA with Collision Avoidance (CSMA/CA) protocol. Although the general idea of CD-MACA is interesting, the definition in [15] is quite general and several implementation details are not considered. From an energy-efficient perspective, another cooperative MAC protocol is also presented within the context of ad hoc networks in [16]. This proposal integrates cooperative diversity into two different wireless routing protocols by embedding a distributed cooperative MAC. In [17] a cooperative MAC protocol was presented within the context of a mesh network formed by an access point, a number of regular stations and one fixed wireless router (helper).

These protocols do not take into account the unique conditions of the MC-ARQ scheme discussed in the previous section, and thus a new field for research is open. We present in the next section the PRCSMA as a MAC protocol conceived to support the concept of C-ARQ and thus easily applicable to a MC-ARQ scheme.

5 Persistent Relay Carrier Sensing Multiple Access (PRCSMA)

The PRCSMA protocol was presented and analyzed in [7] and [8], respectively, with the primary design goal of enabling devices equipped with CSMA-based wireless interfaces to cooperate within their surrounding grid upon the occurrence of a transmission error. Although it was originally designed within the context of C-ARQ schemes, it can be applied for the coordination of the helpers within the short-range interface of a MC-ARQ scheme.

The protocol works as follows: whenever a data packet from a source is received with unrecoverable errors at destination, a cooperation phase can be initiated. A CFC packet is broadcast after sensing the channel idle for a Short Inter Frame Silence (SIFS) period. Regular data transmissions in IEEE 802.11 are done after a longer silence period (Distributed IFS, referred to as DIFS), and thus cooperation phases have higher priority than regular data traffic. The CFC packet invites all the devices to become active helpers as long as they meet some predefined helper selection criteria, which are not specified in the basic definition of PRCSMA. It is worth mentioning that although the optimal scheme would consist in selecting the best helper for each cooperation phase, the approach in PRCSMA is to select a set of the most appropriate active helpers in order to loosen the requirement of selecting exactly the best candidate in each moment. An interesting open line of research might be focused on assessing the trade-off between the costs of selecting the best helper and the time required to solve the contention among a set of selected helpers.

Upon the reception of the CFC packet, all the devices which become active helpers get ready to forward their cooperative information. The specific PHY forwarding strategies applied at the helpers and the reconstructing mechanism implemented at the destination are out of the scope of the basic definition of PRCSMA. Therefore, without loss of generality, the packet transmitted by any helper will be referred to as a cooperative packet. Accordingly, the active helpers will try to get access to the channel in order to persistently transmit their cooperative packets. To do so, the MAC rules specified in the Distributed Coordination Function (DCF) of the IEEE 802.11 standard are used, considering the two following modifications:

1. There is no expected ACK associated to each transmitted cooperation packet.
2. Since the sub-network formed by the helper set works in saturation conditions, i.e., all the helpers have a data packet ready to be transmitted, it is necessary to

execute a backoff mechanism at the beginning of the cooperation phase in order to avoid a certain initial collision. Therefore, those active helpers which do not have an already set backoff counter (from a previous transmission attempt) set it up and initiate a random backoff period before attempting to transmit for the first time. On the other hand, those helpers which already have a non-zero backoff counter value keep the value upon the initialization of a cooperation phase.

A cooperation phase is ended whenever either the destination is able to decode the original data packet by properly combining the different cooperative packets received from the helper set or a certain maximum cooperation timeout has elapsed. In the former case, i.e., a successful cooperation phase, an ACK packet is transmitted by the destination. In the latter case, i.e. if the original packet could not be decoded, a negative ACK (NACK) is transmitted by the destination station. In any case, all the helpers pop-out the cooperative packet from their queue upon the end of a cooperation phase.

According to all this operation, three implementation issues should be considered:

1. The CFC packet can be implemented with a regular RTS packet but using one of the reserved control subtypes to distinguish the packet from a normal RTS, as already done in [12].
2. As long as there is at least one active helper, the persistent behavior of PRCSMA eliminates the probability that the destination does not receive the required amount of local retransmissions by pretending there are infinite devices trying to cooperate.
3. The active helpers could execute either the basic or the collision avoidance (with RTS/CTS handshake) access mode during a cooperation phase. On the one hand, as data bit rates become higher, it becomes more critical to reduce the overhead associated to the payload in order to avoid an unnecessary waste of the radio resources; therefore, it would be desirable to use the basic access mode. However, the collision avoidance mechanism acts as a protection against the hidden terminal problem, and thus it will be mandatory in multi-hop networks.

6 Performance Evaluation

In order to assess the performance of the protocol, link level simulations for a cellular network combined with a WLAN system have been carried out. Due to the complexity of simulating such a hybrid scenario, we have decided to implement an isolated layout in a custom-made MATLAB simulator. A group of wireless nodes, all within the transmission range of each other, are associated to a distant BS. We consider that they are all equipped with both cellular and WLAN interfaces. In order to focus on the MAC evaluation and to avoid obscuring the results with other parameters such as the channel impairments or network topology effects, we have considered a pessimistic worst-case scenario. The downlink between the BS and one predetermined and fixed destination device is in bad conditions and all data packets are received with unrecoverable errors. Therefore, this destination requests cooperative retransmissions from the wireless grid upon the reception of any original data packet from the BS. We consider a saturated condition where the BS always has at least one data packet (with a constant length of 1500 bytes) to transmit. The data and control transmission rates (for the ACK packets with a constant length of 34 bytes, as in the IEEE 802.11 [9]) from the BS to the destination user are both set to a constant value of 6 Mbps.

The short-range network surrounding the destination device is formed by 10 active helpers, all of them within the transmission range of each other. These helpers execute PRCSMA to get access to the channel. They use the basic access method of the protocol, i.e., without RTS/CTS handshake. We assume that the data rates between the helpers and the destination for data and control transmissions are 54 and 6 Mbps, respectively. The initial size of the contention window has been set to 32. The throughput, defined as the number of error-free payload bits (including coding bits) transmitted per second, of the cellular interface is illustrated in Figure 5. The curves represent the throughput as a function of the number of retransmissions required to decode a data packet that has been received with unrecoverable errors. The throughput of three different retransmission schemes is represented:

1. The traditional ARQ curve represents the throughput of the cellular interface in the case that upon transmission error, retransmissions are requested from the BS. Retransmissions are performed one after another until the destination is able to decode the packet without errors and acknowledge its reception.
2. The MC-ARQ curve represents the saturation throughput of the cellular interface in the case that the MC-ARQ scheme with the PRCSMA protocol is executed. In this case, retransmissions are performed through the short-range interface and thus data communication in the cellular link can continue without interruption.
3. The C-ARQ curve represents the saturation throughput of the cellular interface in the case that a C-ARQ scheme is executed within the cellular interface (also executing the PRCSMA at the MAC layer).

It is possible to infer from Figure 5 that as the number of required retransmissions increases, the performance of the C-ARQ scheme outperforms the traditional non-cooperative ARQ scheme. Despite the extra overhead associated to the coordination among the helpers in the short-range network, the higher transmission rate between the helpers and the destination pays off the increased overhead. What results more interesting from the figure is that, if we eliminate retransmissions from the cellular interface, i.e., by means of the MC-ARQ scheme, then the throughput can reach the maximum theoretical performance of the network independently of the number of retransmissions needed. Under the considered PHY layer, this saturation throughput is of 5.7 Mbps (assuming that the only control information exchanged is composed of the ACK packets after each data packet transmission). Comparing this value with the curves from the C-ARQ and the traditional non-cooperative ARQ schemes, we see that the relative performance improvement between the different retransmission schemes becomes higher as the number of needed retransmissions grows. It seems reasonable to believe that this performance may be affected by the number of active helpers. To evaluate its impact, the average packet transmission delay of PRCSMA is represented in Figure 6 as a function of the number of active helpers within the grid, and for different number of required retransmissions (K). This delay is defined as the time elapsed since the moment a packet is first eligible for transmission until K retransmission from the relays are received. The curves show that given a number of required retransmissions, the average packet transmission delay remains almost independent of the number of active helpers. This is a key feature of the PRCSMA protocol which makes it suitable for this kind of communication schemes.

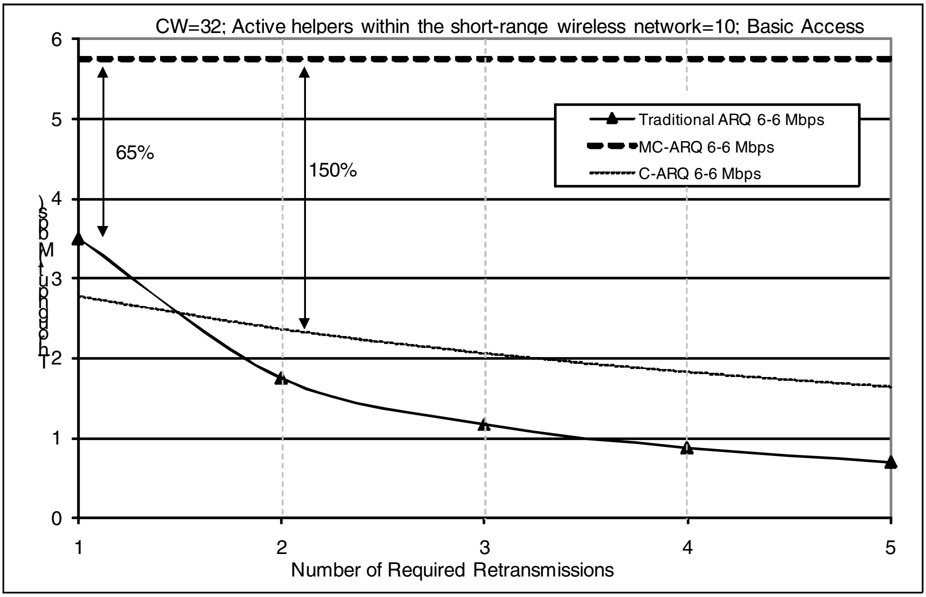


Fig. 5. Throughput in the cellular network

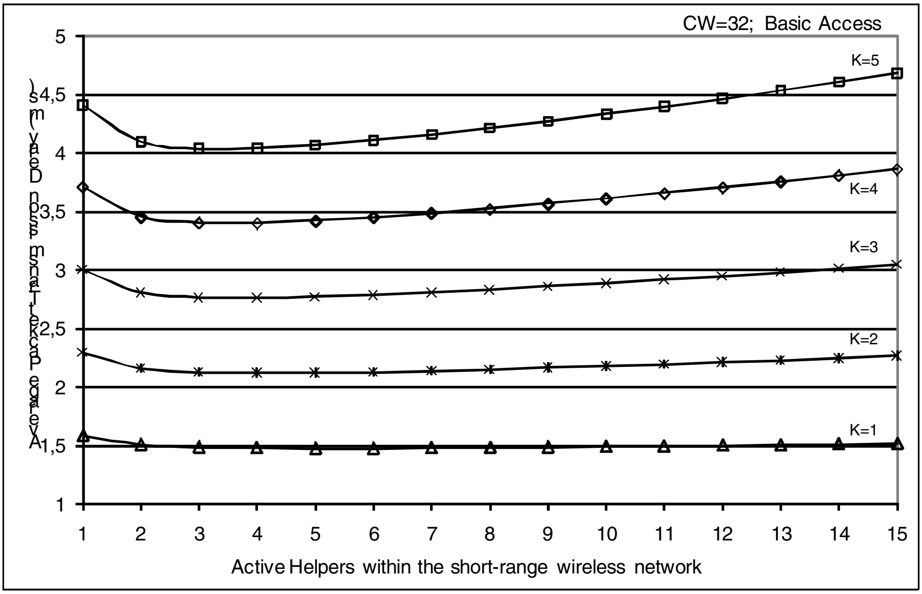


Fig. 6. Average Packet Transmission Delay of PRCSMA for different number of retransmissions (K)

7 Conclusions

The increasing pervasive deployment of wireless devices equipped with several interfaces enables the rise of new communication paradigms. Wireless grids come up as a solution to integrate different wireless interfaces. In this paper we have presented Multi-Radio distributed Cooperative Automatic Retransmission Request (MC-ARQ) schemes as an approach to exploit the potential benefits of wireless grids. The main idea is that whenever a packet is received with errors within a cellular interface (infrastructure-based interface), retransmissions can be requested to neighboring stations which may have received an uncorrelated copy of the original transmission. These retransmissions can be performed through a short-range wireless interface reducing the occupation of the cellular links, improving the usage of the spectrum and reducing the overall average transmitted power.

In order to bring to life this promising concept it is still necessary to study it from different points of view. We have discussed in this paper the unique conditions that this kind of communication schemes poses to the MAC layer. In addition, we have identified PRCSMA as a MAC protocol suitable for the execution of the MC-ARQ scheme in a wireless network without degrading the performance of the cellular interface upon transmission error. Simulation results for a hybrid cellular/WLAN network are promising. In the worst-case example presented in this paper, the data throughput is improved by 65% when compared to traditional non-cooperative ARQ schemes if only one retransmission is required from the grid. This improvement factor grows as the number of required retransmissions increases. In this paper we have focused on the throughput performance. However, it remains as an interesting topic for research how the use of a MC-ARQ scheme may yield benefits in terms of reduced interference as well as energy consumption due to the lower transmission power required for the short-range transmissions. Therefore, the MC-ARQ scheme presented in this paper opens a wide range of interesting research topics to be covered in the upcoming years, and it constitutes a simple and practical approach to apply cooperation in real networks.

Acknowledgment

This work has been partially funded by the Research Projects NEWCOM++ (ICT-216715), R2D2 (CP6-013), CENTENO (TEC2008-06817-C02-02), PERSEO (TEC2006-10459/TCM), COOLNESS (218163-FP7-PEOPLE-2007-3-1-IAPP) and by Generalitat de Catalunya (2009-SGR-940).

References

1. Cover, T.M., Gamal, A.E.: Capacity Theorems for the Relay Channel. IEEE Transactions on Information Theory 25(5), 572 (1979)
2. Sendonaris, A., Erkip, E., Aazhang, B.: Station Cooperation Diversity-Part I: System Description. IEEE Transactions on Communications 51(11), 1927–1938 (2003)

3. Laneman, J.N., Tse, D.N.C., Wornell, G.W.: Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior. IEEE Transactions on Information Theory 50(12) (2004)
4. Fitzek, F.H.P., Katz, M.D.: Cooperation in Wireless Networks: Principles and Applications. Springer, Heidelberg (2006)
5. Fitzek, F.H.P., Katz, M., Zhang, Q.: Cellular Controlled Short-Range Communication for Cooperative P2P Networking. In: Wireless Research Forum (WWRF) 17, Heidelberg, Germany, WWRF, vol. WG 5 (2006)
6. Zimmermann, E., Herhold, P., Fettweis, G.: The Impact of Cooperation on Diversity-Exploiting Protocols. In: Proc. of the 59th IEEE Vehicular Technology Conference (2004)
7. Alonso-Zárate, J., Kartsakli, E., Verikoukis, C., Alonso, L.: Persistent RCSMA: A MAC Protocol for a Distributed Cooperative ARQ Scheme in Wireless Networks. EURASIP Journal on Advanced Signal Processing, Special Issue on Wireless Cooperative Networks 2008, article ID 817401, 13 (2008)
8. Alonso-Zárate, J., Alonso, L., Verikoukis, C.: Performance Analysis of a Persistent Relay Carrier Sensing Multiple Access Protocol. IEEE Transactions on Wireless Communications 8(12) (2009)
9. IEEE, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.-11-99 (1999)
10. IEEE, Part 15.4: Wireless MAC and PHY layer specifications for low-rate wireless personal area networks, IEEE Std. 802.15.4-2006 (2006)
11. Liu, P., Tao, Z., Panwar, S.: CoopMAC: A Cooperative MAC for Wireless LANs. IEEE Journal on Selected Areas on Communications 25(2) (2007)
12. Korakis, T., Natayanan, S., Bagri, A., Panwar, S.: Implementing a Cooperative MAC Protocol for Wireless LAN. In: Proc. of the IEEE International Conference on Communications (ICC 2006), vol. 10, pp. 4805–4810 (2006)
13. Tao, Z., Korakis, T., Slutskiy, Y., Panwar, S., Tassiulas, L.: Cooperation and Directionality: A Coop-directional MAC for Wireless Ad Hoc Networks. In: Proc. of the WiOpt (2007)
14. Shankar, S., Chou, C., Ghosh, M.: Cooperative Communication MAC (CMAC) – A new MAC protocol for Next Generation Wireless LANs. In: Proc. of the IEEE International Conference on Wireless Networks, Communications and Mobile Computing (2005)
15. Wang, X., Yang, C.: A MAC Protocol Supporting Cooperative Diversity for Distributed Wireless Ad Hoc Networks. In: Proc. of the IEEE International Symposium on PIMRC, Berlin, Germany (2005)
16. Azgin, A., Altunbasak, Y., Alrebig, G.: Cooperative MAC and Routing Protocols for Wireless Ad Hoc Networks. In: Proc. of the IEEE Globecom (2005)
17. Sadek, A., Ray Liu, K.J., Ephremides, A.: Collaborative Multiple-Access Protocols for Wireless Networks. In: Proc. of the IEEE International Conference on Communications, ICC 2006 (2006)

Joint Turbo Coding and Source-Controlled Modulation of Cycle-Stationary Sources in the Bandwidth-Limited Regime

Idoia Ochoa[1], Pedro M. Crespo[1], Javier Del Ser[2], and Mikel Hernaez[1]

[1] CEIT and TECNUN (University of Navarra), 20009 San Sebastian, Spain
`{iochoa,pcrespo,mhernaez}@ceit.es`
[2] TECNALIA-TELECOM, 48170 Zamudio, Spain
`jdelser@robotiker.es`

Abstract. In this paper we propose a novel one-layer coding/shaping transmission system for the bandwidth-limited regime based on single-level codes and sigma-mapping [1]. Specifically, we focus on cycle-stationary information sources with independent symbols. High spectral efficiencies can be achieved by combine at the transmitter a Turbo code with a sigma-mapper. Furthermore, the encoded symbols are modulated by using an asymmetric energy allocation technique before entering the aforementioned sigma-mapper. The corresponding decoder iterates between the Turbo decoder and the sigma-demapper, which exchange progressively refined *extrinsic* probabilities of the encoded symbols. For the Additive White Gaussian Noise (AWGN) channel, simulation results obtained for very simple Turbo codes show that the proposed system attains low bit error rates at signal-to-noise ratios relatively close to the corresponding Shannon limit. These promising results pave the way for future investigations towards reducing the aforementioned energy gap, e.g. by utilizing more powerful Turbo codes.

Keywords: Turbo codes, sigma-mapping, bandwidth-limited regime, unequal energy allocation, cycle-stationary sources.

1 Introduction

We consider the transmission, over the Additive White Gaussian Noise (AWGN) channel, of binary symbols generated by cycle-stationary random processes, $\{T_k\}_{k=1}^{\infty}$, with independent symbols. This kind of processes may arise, for instance, when the output sequence generated by a binary stationary source with memory[1] is partitioned into blocks of K symbols, before being processed by the block-sorting Burrows-Wheeler Transform (BWT) [2] of length K. For large K, it can be shown [3] that the corresponding random process $\{T_k\}_{k=1}^{\infty}$ at the output of the BWT can be asymptotically approximated by a cycle-stationary

---

[1] A source with memory may be modeled by either a Markov Chain (MC) or a Hidden Markov Model (HMM).

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 618–625, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

random process with time period K (i.e. the length of the BWT input block), and independent symbols inside each output block. Under these conditions, the output process is completely specified once the probability distribution of each of the symbols inside an arbitrary block, say the first block, are known, i.e., when $P_{T_k}(t)$, for $k = 1, \ldots, K$ are known. Notice that the random sequence $\{T_k\}_{k=1}^{K}$ is non-stationary.

The entropy rate of such a process can be computed as

$$\mathcal{H}(\mathcal{T}) = \lim_{n\to\infty} \frac{1}{nK} H(T_1, \ldots, T_{nK}) = \frac{1}{K} H(T_1, \ldots, T_K) = \frac{1}{K} \sum_{k=1}^{K} H(T_k), \tag{1}$$

where $H(T_1, \ldots, T_K)$ denotes the entropy of the random vector $\{T_k\}_{k=1}^{K}$ with joint distribution $P_{\mathbf{T}}(t_1, \ldots, t_K) = \prod_{k=1}^{K} P_{T_k}(t_k)$. In what follows, we will denote by $P^0(k) = P_{T_k}(t = 0)$, and the set of values $\{P^0(k)\}_{k=1}^{K}$ inside a non-stationary block will be referred to as the *zero probability profile*. Notice that by cycle-stationarity $P^0(lK + k) = P^0(k)$, $\forall l \in \mathbb{N}$.

By the Shannon Source-Channel Coding Theorem [4], the minimum average energy per source symbol E_{so} required for reliable communication of $\{T_k\}_{k=1}^{\infty}$ over an AWGN channel is given by

$$\frac{E_{so}}{N_0} > \frac{2^{2R\mathcal{H}(\mathcal{T})} - 1}{2R}, \tag{2}$$

where N_0 is the one-sided noise power spectral density, R denotes the transmission rate (source symbols per channel symbol), and $2R$ is the spectral efficiency (binary source symbols per two dimensions). When the system has a spectral efficiency equal or greater than 2, it operates in the bandwidth-limited regime. Otherwise, it is said that the system works in the power-limited regime.

By the Separation Theorem, the lower limit in expression (2) can be achieved by an ideal source encoder followed by a capacity achieving channel code. However, in this paper we propose a novel scheme, suitable for the bandwidth-limited regime, which do not use a source encoder but rather uses the distribution $P^0(k) \doteq P_{T_k}(t = 0)$ (*zero probability profile*) of the source symbols T_k to modify the BPSK constellation at the output of the Turbo encoder before entering the sigma-mapper [1]. In this context, the present paper can be viewed as an extension of the scheme proposed in [5], suitable in the power-limited regime, for the transmission of the symbols generated by a stationary source with memory over the AWGN channel. Preliminary simulation results with very simple Turbo codes show a Bit Error Rate performance relatively close to the associated Separation limit, which sets the scene for future research aimed at narrowing this performance gap.

The rest of the paper is organized as follows: Section 2 and 3 describe the encoding and decoding process, respectively. Simulation results are presented in Section 4, and finally, some concluding remarks are drawn in Section 5.

2 Encoding Process

Figure 1 shows the proposed system, which combines Turbo coding and shaping in a one-layer scheme. The cycle-stationary source $\mathcal{T}$ of period K, generates blocks of K independent symbols $\{T_k\}_{k=1}^{K}$ having a *zero probability profile* $\{P^0(k)\}_{k=1}^{K}$. The source symbols are first encoded by a Turbo code of rate $R_c = K/N$. The encoded sequence $\mathbf{c}$ of length N is next interleaved to form the sequence $\tilde{\mathbf{c}}$ of the same length. The interleaved block $\tilde{\mathbf{c}}$ is then transformed by a serial-to-parallel converter in $\mathcal{I}$ sequences $\mathbf{v}^{(i)}$ of length L, where $0 \leq i \leq (\mathcal{I}-1)$ and $N = L \cdot \mathcal{I}$.

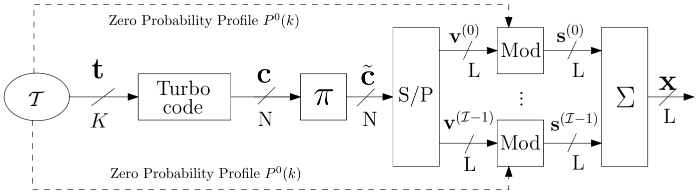


Fig. 1. Proposed transmission scheme

Before entering the sigma-mapper, the modulator assigns different amplitudes to the encoded symbols, depending on their position and their systematic or parity nature. The proposed energy allocation scheme (further detailed in Subsection 2.1) renders a set of $\mathcal{I}$ non-binary sequences $\mathbf{s}^{(i)}$, which are next fed to the sigma-mapper Σ [1]. The underlying idea of the sigma-mapper hinges on imposing a gaussian distribution on the output amplitude signal $\mathbf{x}$ of length L while satisfying, at the same time, the energy constraint[2] $(1/L) \cdot \sum_{l=1}^{L} \mathbb{E}\{|X_l|^2\} = E_c$. Finally, the destination receives a corrupted version of the amplitude sequence $\mathbf{x}$, denoted as $\mathbf{y} = \mathbf{x} + \mathbf{n}$, where $\mathbf{n}$ denotes a L-length sequence of i.i.d. Gaussian random variables with zero mean and variance per dimension $N_0/2$.

2.1 Asymmetric Energy Allocation Scheme

From expression (2), the minimum average energy per channel symbol E_c for reliable communication of the data generated by the binary cycle-stationary source $\mathcal{T}$ is given by[3]

$$\frac{E_c}{N_0} > \frac{2^{2R\mathcal{H}(\mathcal{T})} - 1}{2}, \tag{3}$$

with

$$\mathcal{H}(\mathcal{T}) \doteq \frac{1}{K} \sum_{k=1}^{K} h_b(P^0(k)), \tag{4}$$

---

[2] $\mathbb{E}\{\cdot\}$ stands for *expectation*.

[3] Notice that in equation (3), R refers to the overall rate of the system, which may differ from R_c (coding rate).

where $h_b(p) \doteq -p\log_2 p - (1-p)\log_2(1-p)$. However, since in our case the symbols inside a block are non-stationary, each output symbol will require a different average energy $E_c(k)$ depending on its distribution $P^0(k)$. From expression (3), the corresponding lower limit will be given by

$$E_c^*(k) = (2^{2Rh_b(P^0(k))} - 1)\frac{N_0}{2}, \tag{5}$$

and the minimum average energy per block as

$$E_c^* = \frac{1}{K}\sum_{k=1}^{K} E_c^*(k). \tag{6}$$

The energies used to modulate the encoded symbols are now given by $E(k) = \beta E_c^*(k)$, for $k = 1, \ldots, K$ where $\beta > 1$ is a scaling factor. Following the scheme of [5], the amplitudes of the encoded systematic symbols depend on both their value and the associated *a priori* probability $P^0(k)$, whereas the amplitude of a given encoded parity symbol is driven by 1) its value and 2) the value and the *a priori* probability of the associated systematic bit. In particular, the amplitudes are set to:

$$\text{Systematic symbols:} \begin{cases} -\sqrt{\frac{1-P^0(k)}{P^0(k)}E(k)}, \text{ if } u_k = 0, \\ +\sqrt{\frac{P^0(k)}{1-P^0(k)}E(k)}, \text{ if } u_k = 1. \end{cases} \tag{7}$$

$$\text{Parity symbols:} \begin{cases} -\sqrt{\frac{\theta}{P^0(k)}E(k)}, \text{ if the parity symbol is 0 and } u_k = 0, \\ -\sqrt{\frac{1-\theta}{1-P^0(k)}E(k)}, \text{ if the parity symbol is 0 and } u_k = 1, \\ +\sqrt{\frac{\theta}{P^0(k)}E(k)}, \text{ if the parity symbol is 1 and } u_k = 0, \\ +\sqrt{\frac{1-\theta}{1-P^0(k)}E(k)}, \text{ if the parity symbol is 1 and } u_k = 1. \end{cases} \tag{8}$$

where the arbitrary parameter θ ($0 \leq \theta \leq 1$) is chosen to maximize the performance of the system, which is usually achieved when $\theta = 0.5$ [6]. In the simulations presented in this paper, θ was set to 0.5. Notice that the resulting constellation is not symmetric, since more energy is allocated to those symbols with less *a priori* probability. Also observe that for the sake of clarity, the above expressions (7) and (8) do not include the time index mappings due to the Turbo and π interleavers, which must be considered in the energy allocation procedure.

A better estimation of the energies $E_c^*(k)$ defined in equation (5) can be obtained by taking into account the loss in performance due to using a non-capacity-achieving channel code, i.e. the actual gap to the corresponding Shannon limit. This is done by introducing, into expression (5), a gap factor $\Gamma(P^0(k))$, i.e.

$$E_c^*(k) = (2^{2Rh_b(P_s^0(k))} - 1)\frac{N_0}{2}\Gamma(P^0(k)). \tag{9}$$

The gap $\Gamma(p)$, $p \leq 0.5$, is a function of the *a priori* probability and depends on the particular communication scheme being used. Its value should be computed off-line by Monte Carlo simulations. Once $\Gamma(\cdot)$ is known, the amplitudes of the encoded symbols are calculated by following expressions (9), (6), (7) and (8), with $E(k) = \beta E_c^*(k)$ for a given scaling factor β.

3 Decoding Process

The decoder is depicted in Figure 2. It iterates between the sigma-demapper, which introduces the *a priori* probabilities of the source symbols, and the Turbo decoder, which is based on applying the message passing Sum-Product Algorithm (SPA) over the factor graph that describes the Turbo code [7].

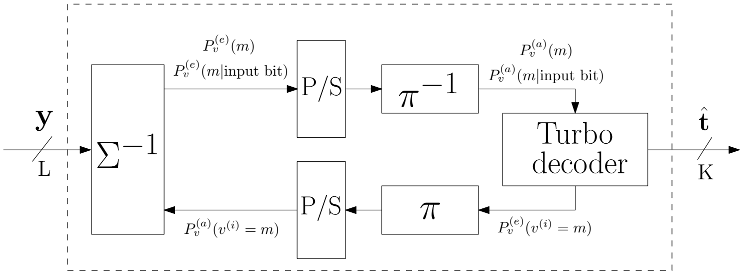
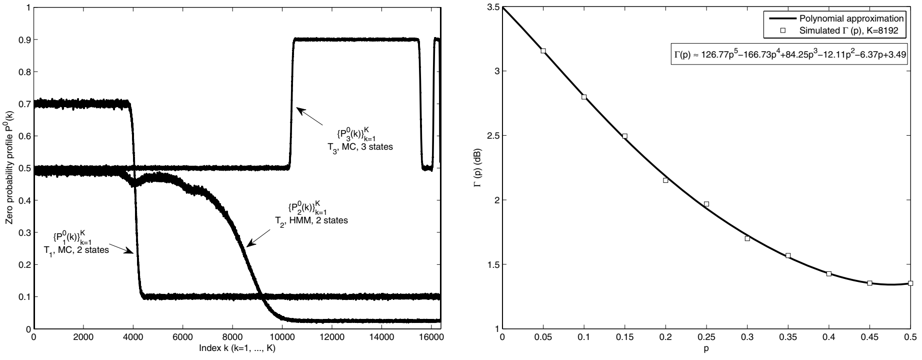


Fig. 2. Decoding scheme

The iterative decoding process starts from the sigma-demapper $\sum^{-1}$, which estimates the probabilities of the symbols contained in each of the $\mathcal{I}$ sequences $\mathbf{v}^{(i)}$ from the received sequence $\mathbf{y}$. These probabilities are denoted by $P_v^{(e)}(m)$ for systematic bits ($m \in \{0, 1\}$), and by $P_v^{(e)}(m|\text{input bit})$ for parity bits. Once these probabilities are computed, the Turbo decoder incorporates them (through the parallel-to-serial converter and the deinterleaver π^{-1}) as *a priori* information on the systematic and parity encoded symbols. Then, the SPA applied to the factor graph of the Turbo code produces a set of refined *a posteriori* and *extrinsic* probabilities[4]; the latter are then fed back to the sigma-demapper as a *a priori* probabilities, giving rise to a new iteration. At each iteration, an estimation $\widehat{T}_k$ of T_k can be obtained for $k = 1, \ldots, K$ by performing a hard-decision over the *a posteriori* probabilities generated by the Turbo decoder. The decoding process is stopped after a fixed number of iterations Ψ. It is important to observe that, in our scheme, the SPA applied to the Turbo factor graph is extended with respect to the conventional forward and backward recursions (see [7, Section IV.A]) so as to incorporate the generation of the *extrinsic* probabilities corresponding to the parity bits.

---

[4] In the Turbo processing jargon, *extrinsic* refers to the fraction of the output probabilistic information that does not depend on any input *a priori* probability.



(a) (b)

Fig. 3. (a) Zero probability profiles of the considered MC and HMM sources concatenated with the BWT, and $K = 16384$. (b) Polynomial approximation of the gap margin functions for the proposed scheme and $K = 8192$.

4 Simulation Results

In order to study the performance of the proposed system, we have considered three different cycle-stationary sources $\mathcal{T}_i$ with *zero probability profiles* $\{P_i^0(k)\}_{k=1}^K$, with $i \in \{1, 2, 3\}$ and $K = 16384$. They have been obtained by estimating the probability distribution at the output of the BWT for an input source with memory following a Markov Chain (MC) for $i \in \{1, 3\}$, and a Hidden Markov Model (HMM) for $i = 2$. For $i = 1$ and $i = 2$, we have utilized the MC and the HMM employed in [5], both having two states and entropy rates 0.58 and 0.62 bits per source symbol, respectively. On the other hand, for $i = 3$ we have selected a MC with 3 states and entropy rate 0.83 bits per source symbol. The corresponding *zero probability profiles* at the output of the BWT are shown in Figure 3.a, which have been estimated by using frequency of occurrence as in [8, Expression (57)]. The Turbo code from [1, Example A] with rate $R_c = 1/3$ and generator polynomial $G(D) = 1/(1 + D)$ has been adopted for our simulations. The serial-to-parallel converter outputs $\mathcal{I} = 3$ sequences $\mathbf{v}^{(i)}$, and therefore the overall transmission rate R (source symbol per dimension) is 1, i.e. we are working in the bandwidth-limited regime (spectral efficiency of 2). The corresponding Shannon limits E_{so}/N_0 when $R = 1$ are -2.13 dB ($\mathcal{T}_1$), -1.69 dB ($\mathcal{T}_2$) and 0.293 dB ($\mathcal{T}_3$).

Figure 3.b depicts the gap factor $\Gamma(p)$, $p \leq 0.5$, used in expression (9). This gap has been calculated by simulating the proposed scheme for a stationary i.i.d. source with symbol distribution $(p, 1-p)$ and blocklength $K = 8192$ (□ markers). The figure also includes a 5^{th}-order polynomial approximation for the simulated $\Gamma(p)$, which can be easily programmed beforehand to produce the gamma function for any arbitrary value of p. Observe that $\Gamma(p)$ is a monotonically decreasing function of p, which indicates that the performance of the proposed setup with

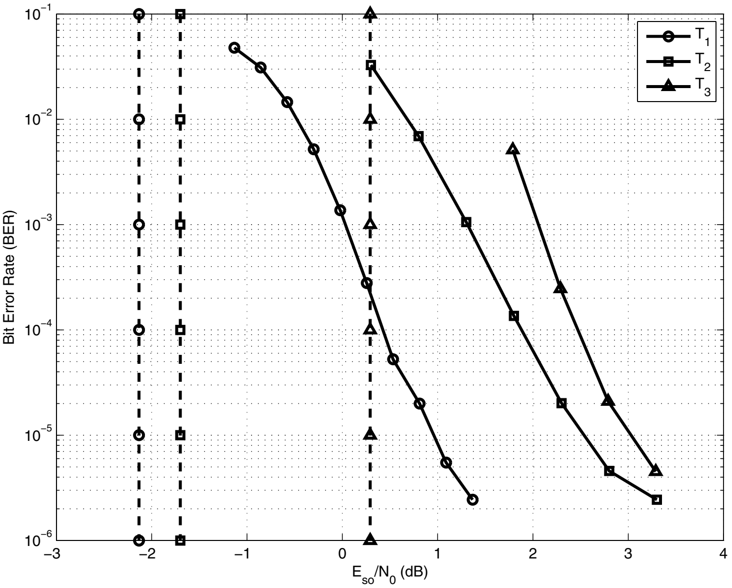


Fig. 4. BER vs E_{so}/N_0 of the proposed scheme for $\{\mathcal{T}_i\}_{i=1}^{3}$

i.i.d. stationary sources degrades as the distribution of the source symbols is more asymmetric.

Finally, Monte Carlo simulations have been performed for a blocklength of $K = 16384$ source symbols, $\Psi = 50$ decoding iterations and 1000 source sequences per simulated point. Figure 4 plots the Bit Error Rate (BER) versus E_{so}/N_0 for the three probability profiles and by using the energy allocation technique introduced in Section 2.1. However, we have modified the way the set of energies $E_c^*(k)$ is calculated, because simulations have empirically shown a performance improvement when R is replaced by R_c in expression (9). When the source is generated with the first probability profile $\{P_1^0(k)\}_{k=1}^{K}$ ($\mathcal{T}_1$), the proposed system is 2.55dB away of the theoretical limit for a BER of 10^{-4}. For the second probability profile ($\mathcal{T}_2$), the system is 3.57 dB away of its corresponding Shannon limit. Finally, the system applied to the third source $\mathcal{T}_3$ performs at 2.17 dB away from the corresponding Shannon limit at the same BER level. Notice that these results have been obtained by means of a very simple Turbo code. We believe that by optimizing the Turbo code better results (i.e. closer to the Shannon limit) could be obtained.

5 Concluding Remarks

We have proposed a novel scheme for the transmission of cycle-stationary sources over AWGN channels in the bandwidth-limited regime. The novel scheme is based on the combination of a Turbo encoder and a sigma-mapper that jointly perform the source and channel coding task, and on the use of an asymmetric waterfilling energy allocation technique. The simulation results obtained for very simple Turbo codes state that, for a variety of cycle-stationary sources, the BER performance of our proposed scheme gets close to the corresponding Shannon separation limit. These promising results motivate further research towards narrowing the aforementioned gap, e.g. by utilizing Turbo codes with enhanced BER waterfall performance.

Acknowledgments

This work was supported in part by the Spanish Ministry of Science and Innovation through the CONSOLIDER-INGENIO 2010 programme (CSD200800010, www.comonsens.org), and through the Torres-Quevedo funding program (PTQ-09-01-00740).

References

1. Ma, X., Ping, L.: Coded Modulation Using Superimposed Binary Codes. IEEE Transactions on Information Theory 50(12) (2004)
2. Burrows, M., Wheeler, D.: A Block Sorting Lossless Data Compression Algorithm, Digital Systems Center, Research Report 124 (1994)
3. Visweswariah, K., Kulkarni, S., Verdu, S.: Output Distribution of the Burrows-Wheeler transform. In: IEEE International Symposium on Information Theory, Sorrento, Italy (2000)
4. Shannon, C.E.: A Mathematical Theory of Communication. Bell System Technical Journal 27, 379–423, 623–656 (1948)
5. Del Ser, J., Crespo, P.M., Esnaola, I., Garcia-Frias, J.: Source-Controlled Turbo Coding of Sources with Memory using the Burrows-Wheeler Transform. In: IEEE International Symposium on Turbo Codes, Munich, Germany (2006)
6. Cabarcas, F., Souza, R.D., Garcia-Frias, J.: Turbo Coding of Strongly Non-Uniform Memoryless Sources with Unequal Energy Allocation and PAM Signaling. IEEE Transactions on Signal Processing 54(5), 1942–1946 (2006)
7. Kschischang, F.R., Frey, B.J., Loeliger, H.-A.: Factor Graphs and the Sum-Product Algorithm. IEEE Transactions on Information Theory 47(2), 498–519 (2001)
8. Crespo, P.M., Loyo, E., Del Ser, J.: Uncoded Optimal Binary Communication for Sources with Memory. Elsevier AEU International Journal of Electronics and Communications 62(8), 597–609 (2007)

Harmony Search Heuristics for Quasi-asynchronous CDMA Detection with M-PAM Signalling

S. Gil-Lopez, J. Del Ser, and L. Garcia-Padrones

TECNALIA-TELECOM
Pt. Tecnológico, Edif. 202, 48170 Zamudio, Spain
`sgil,jdelser@robotiker.es`

Abstract. Focusing on CDMA (Code Division Multiple Access) uplink communications, this paper addresses the application of heuristic techniques to the multiple user detection problem when dealing with asynchrony between transmitters and bandwidth-limited PAM (Pulse Amplitude Modulation) signals. In such systems it is known that, even for the simplest case of binary modulated signals with perfectly synchronous transmitters, simple Single-User Detection (SUD) techniques (e.g. Rake receiver) are outperformed by Multiple-User Detection (MUD) schemes (based on the Maximum-Likelihood – ML – criteria), at a computational cost exponentially increasing with the number of users. Consequently, Genetic Algorithms (GA) have been extensively studied during the last decade as a means to alleviate the computational complexity of CDMA MUD detectors while incurring, at the same time, in a negligible error rate penalty. In this manuscript, a novel heuristic approach inspired in the recent Harmony Search algorithm will be shown to provide a faster convergence and a better error rate performance than conventional GA's in presence of inter-user asynchrony in bandwidth-limited CDMA communications, specially when the complexity of the scenario increases.

Keywords: CDMA, Multi-user Detection, Genetic Algorithm, Harmony Search.

1 Introduction

From the beginning of wireless communication systems in the late 1970's, huge research has been conduced towards designing efficient transmission and reception techniques aimed at providing ever-growing capacity and/or end-to-end Quality of Service (QoS). A wide variety of problems related to the design and optimization of wireless networks constitute, by themselves, NP-hard problems [1], such as the design of TDMA (Time Division Multiple Access) frame patterns [2], data equalization in dispersive links [3], channel estimation [4], topology design [5], terminal assignment [6] and the Access Node Location Problem (ANLP) [7,8], among others. In NP-hard problems, the dimension of the solution space increases exponentially with the number of inputs, and consequently they cannot be solved in

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 626–637, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

polynomial time. Consequently, achieving exact optimum solutions is not feasible in practical scenarios with underlying NP-hard optimization problems.

One of such problems related to wireless communication networks hinges on the joint detection of the data sent by several users over a multiple access channel (also referred to as *uplink* communications). Different multiple access methods have been thoroughly proposed in the literature aimed at separating the signals from the users in some domain, e.g. TDMA (Time), FDMA (Frequency), SDMA (Spatial) and CDMA (Code Division Multiple Access). Let us focus on the latter, where different nodes simultaneously share the channel resources by solely multiplying their data by a set of spreading codes (Figure 1). Note that at reception, the performance of these systems depends roughly on both the method employed to separate the data coming from each node and the orthogonality properties of the set of utilized codes. For instance, the simplest Single-User Detection (SUD) technique just multiplies the received multiplexed signal by the code corresponding to the desired node, which involves considering the signals from undesired nodes (*Multiple Access Interference*, MAI) as noise and, ultimately, an increased effective noise variance. On the contrary, joint Multiple-User Detection (MUD) schemes treat the aforementioned MAI as information rather than noise, which dramatically enhances the error performance of the system at the expense of incrementing the computational complexity of the detection procedure. In this context, the optimum Maximum Likelihood (ML) detector was first proposed by Verdú in [9], whose most elementary implementation is based on exhaustively searching over all possible combinations of the symbols transmitted by the nodes/users. This specific ML search procedure maximizes the computational complexity of the detector exponentially with the number of nodes in the network, hence constituting by itself a NP-hard problem.

For this reason, the research on this field has significantly been devoted to novel optimized heuristic and/or stochastic MUD search procedures offering a good balance between error performance and computational complexity. Juntti *et al* were the first to propose a Genetic Algorithm as an alternate MUD approach [10], work which unchained a plethora of GA-inspired techniques aimed at jointly detecting multiple users in several instances of CDMA networks (e.g. see [11,12,13,14] and references therein). Such genetic algorithms can be regarded as a class of evolutionary methods which employs the natural selection process as a global search technique. In these algorithms the proposed potential solutions are represented by chromosomes so as to constitute the different individuals of the population. The algorithm operates in an iterative manner to produce new generations (i.e. sets of potential solutions) by mimicking the processes of selection, crossover and mutation involved in the natural evolution in species and organisms. The population is updated if new proposed candidate solutions are better – under a certain fitness or cost function evaluation – than those corresponding to previous generations. The above iterative processes are repeated until a termination criterium is satisfied.

Following this research trend, this paper proposes the adaptation of the recent Harmony Search (HS, see [15]) heuristic algorithm to the CDMA MUD

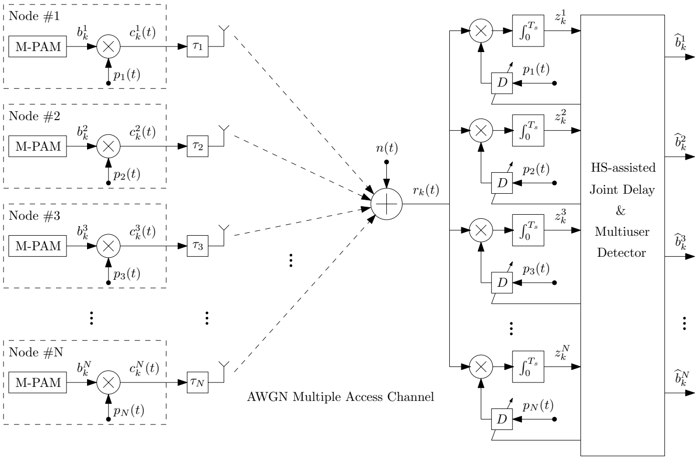


Fig. 1. Block diagram of the N-node quasi-asynchronous CDMA uplink model

detection problem. The HS algorithm mimics the behavior of a music orchestra in the process to compound an harmonious melody, and has been successfully applied to different optimization problems such as water network design [16], multicast routing [17] or even solving the *Sudoku* puzzle [18]. Surprisingly, HS has attracted very marginal attention within the engineering community; to the authors' knowledge, only the recent, independent and almost simultaneous contributions in [19,20] have considered the application of HS to binary-modulated CDMA Multiple-User Detection. The work presented here takes a step further and compares the behavior of a classical Genetic Algorithm and the novel Harmony Search in two CDMA uplink scenarios: 1) quasi-synchronous BPSK modulated transmitters, and 2) M-PAM modulated synchronous transmission. Exhaustive computer simulations conclude that, for a given maximum number of iterations and all the simulated scenarios, HS outperforms GA in terms of end-to-end symbol error rate, specially when the dimension of the solution space increases.

The rest of the manuscript is organized as follows: the mathematical description of the considered CDMA scenarios is presented in Section 2, whereas Section 3 outlines the main characteristics of the proposed HS-based CDMA MUD algorithm. Next, in 4 a comparison study between the algorithms is presented in terms of Symbol Error Rate (SER) and computational complexity. Finally, Section 5 draws some concluding remarks.

2 System Description

We assume the system depicted in Figure 1, i.e. a CDMA network consisting of N nodes which transmit statistically independent data to a common destination. In an equivalent low-pass representation, at time k the n-th node ($n \in \{1, \ldots, N\}$)

generates a M-ary PAM modulated symbol $b_k^n \in \mathcal{B}_M$ at a symbol rate $1/T_s$ symbols/second, where $\mathcal{B}_M \triangleq \{2z-M-1,\, z=1,\ldots,M\}$. Following the previous low-pass representation, each original node symbol b_k^n is CDMA-encoded by using the local signature sequence $p_n(t)$ of duration LT_c, where T_c denotes the chip period. The equivalent low-pass transmitted signal at node n and time k will be therefore given by $c_k^n(t) = b_k^n p_n(t)$. All the nodes' signals are sent over an AWGN multiple access channel, yielding the overall received sequence

$$r_k(t) = \sum_{n=1}^{N} c_k^n(t-\tau_n) + n(t), \tag{1}$$

where $n(t)$ is an additive white random process with zero mean and spectral density amplitude $N_0 = 2\sigma^2$. Note that the transmitted signal at each node n is subject to a random time delay $\tau_n = \xi_n T_c$ ($\xi_n \in \mathbb{N}$). For sake of simplicity we will further assume that $(\max \tau_n) + LT_c < T_s$, i.e. no inter-symbol interference due to temporal delay overlapping is considered in our setup. Observe that this assumption yields $0 \leq \xi_n \leq L-1$ for $n \in \{1,\ldots,N\}$. No a priori information on the delays $\{\tau_n\}_{n=1}^N$ is considered at the sensors or at the common receiver.

At destination, the simplest CDMA SUD (*Single User Detector*) detection strategy would process the received signal $r_k(t)$ through a cascade of $N \cdot L$ matched filters. Each of such filter stages would separate the contribution from each node $n \in \{1,\ldots,N\}$ to the received signal by assuming a certain delay associated to the node at hand. The output ρ_n^l associated to the $((n-1)\cdot L + l)^{th}$ matched filter ($n \in \{1,\ldots,N\}$ and $l \in \{0,...,L-1\}$) would be given by

$$\rho_n^l = \int_0^{T_s} r_k(t) \cdot p_n(t - lT_c), \tag{2}$$

from which the symbol estimation $\widehat{b}_k^n$ for the transmitted symbol b_k^n would be obtained as $\widehat{b}_k^n = \mathrm{HD}_{\widetilde{\mathcal{B}}}[\max_l \rho_n^l]$, with $\mathrm{HD}_{\widetilde{\mathcal{B}}}$ denoting *hard decision* over the constellation $\widetilde{\mathcal{B}} \triangleq \{2Lz - ML - L,\, z=1,\ldots,M\}$. Despite its simplicity, in this SUD detection technique the information contributed by each node to the received sequence $r_k(t)$ is processed without taking into account the contribution of the information from the other nodes, which ultimately leads to a poor end-to-end performance with dramatically high error floors. This gets even more involved in scenarios with strong Multiple Access Interference (MAI), e.g. when utilizing pseudo-random non-orthogonal spreading sequences and fully-loaded (i.e. $N \approx L$) CDMA setups.

As a means to enhance the performance of the SUD receiver, the optimum Maximum Likelihood (ML) receiver estimates $\mathbf{b}_k \triangleq \{b_k^n\}_{n=1}^N$ as $\widehat{\mathbf{b}}_k$ by maximizing the conditional probability

$$\widehat{\mathbf{b}}_k = \underset{\mathbf{b}_k \in \mathcal{B}^N}{\arg\max}\, Pr\left\{\mathbf{b}_k | z_k^1(\tau_1),\ldots,z_k^N(\tau_N)\right\}, \tag{3}$$

where $z_k^n(\tau_n)$ denotes the output of the decorrelator matched to the sequence $p_n(t-\tau_n)$. Observe that if $\tau_n = 0$ for all n (synchronous CDMA setup), the above expression reduces to the classical CDMA decision rule [21]

$$\tilde{\mathbf{b}}_k = \arg\min_{\mathbf{b}_k \in \mathcal{B}^N} \left(\text{-}\, 2\mathbf{b}_k^H \mathbf{z}_k + \mathbf{b}_k^H \mathbf{R} \mathbf{b}_k \right), \tag{4}$$

where $\mathbf{R}$ denotes the $N \times N$ nonnegative definite cross-correlation matrix between spreading code sequences, and ^{H} denotes hermite conjugate. Unfortunately, even for the simplest case of fully-synchronous transmitters the implementation of the decision rule in expression (4) involves a NP-hard optimization problem which requires evaluating the above metric for $|\mathcal{B}|^N = M^N$ distinct candidate vectors. When turning to the asynchronous case, the search space is further extended to cover, not only all possible symbol vectors $\mathbf{b}_k$, but also all the possible combinations of time delays $\{\tau_n\}$. Therefore, the complexity of an exhaustive search ML detection method is increased by a multiplicative factor $(\xi_{\max})^N$, with $\xi_{\max} \triangleq \max_{n=1,\ldots,N} \xi_n$.

3 Harmony Search CDMA Detector

In order to reduce the computational complexity of the exhaustive search based ML detector, we propose to jointly estimate the symbols sent by the different nodes and the set of corresponding delays $\{\tau_n\}_{n=1}^N$ by means of the Harmony Search (HS) heuristic technique [15]. In general, Harmony Search is a heuristic optimization algorithm based on mimicking the behavior of a music orchestra in the process of seeking the best harmony. In this process a set of candidate solutions or *harmonies* (known as *Harmony Memory*) is evaluated under an aesthetic point of view in much the same way as it is done with the population of *chromosomes* in a standard Genetic Algorithm. The Harmony Memory contains a set of φ harmonies which are iteratively updated in an heuristic fashion until a fixed number of attempts is reached or, alternately, a convergence constraint is met[1]. Regarding the system considered in this paper, and following the nomenclature related to the HS algorithm, we will hereafter refer to a given candidate vector $\mathbf{b}_k \in \mathcal{B}^N$ as *harmony*, whereas each compounding entry b_k^n of $\mathbf{b}_k$ will be denoted as *note*.

In the standard implementation of the HS algorithm by Geem *et al* [15], the improvisation process of the new harmonies is made note by note for all harmonies included in the Harmony Memory. At each iteration, the first improvisation criteria establishes that the new value for a note inside a given harmony can be drawn, with a tunable probability, from the values taken by such note in all the other $\vartheta - 1$ harmonies. In a second step, a fine adjusting pitch over the note vocabulary (also driven by an adjustable probabilistic parameter) is performed on every note of the harmony memory. A third random process allows for the heuristic recovery of note values that could have been lost during the previous steps of the improvisation process. In the last step of each iteration, a new improvised harmony is included in the harmony memory if its metric is better than any of the harmonies remaining from the previous iteration.

---

[1] One could use metric thresholding or monitor the uniformity of the Harmony Memory to that end, for instance.

In the scenario considered in this manuscript the HS based detection algorithm works sequentially with two distinct harmony memories: the first set of φ N-dimensional harmonies corresponds to the candidate symbol vectors $\mathbf{b}_k$, whereas each N-dimensional harmony contained in the second memory represents a combination of time delays expressed as an natural multiple of the chip period T_c. The main idea of the proposed sequential HS procedure is based on iterating between the symbol harmony memory and the time delay harmony memory, and on applying, at each iteration, an individual HS improvisation procedure onto each of such memories. Notice that the i-th time delay harmony ($i \in \{1, \ldots, \varphi\}$) allows for the computation of the matched filters' outputs $\{z_k^n(\tau_n)\}_{n=1}^N$, which will then utilized for computing the i-th metric in the righthand expression of equation (3). In other words, the i-th potential solution of the proposed algorithm will be composed of the i-th harmonies of both the symbol and delay memories.

To be concise, the algorithm flow diagram is depicted in Figure 2, and consists of four steps:

A. The **initialization** process is only executed at the first iteration. At this point, if no a priori knowledge of the solution is assumed, the harmonies of both the symbol and the time delay memories are filled randomly with notes drawn from the corresponding alphabet (i.e. $\mathcal{B}$ for the symbol notes and $\{0, \ldots, L-1\}$ for the time delay notes). It should be made clear that, although the initialization is essential for the performance of the algorithm, in this paper we assume the worst scenario where no a priori knowledge on the best harmonies is considered. Otherwise, the performance of our approach will be significantly improved.

B. Next, the **improvisation** process is sequentially applied to each note of the complete set of symbol and delay harmonies, but note that the metric of the proposed solution is evaluated just φ times per iteration. The proposed method is controlled by three arbitrary parameters, as opposed to the nominal algorithm where only two are used:
   - The Harmony Memory Considering Rate, HMCR $\in [0,1]$, which establishes the probability that the new value for a note belonging to a given harmony is drawn from the values of the same note in all the other $\varphi - 1$ harmonies in the respective memory.
   - In the present scheme, the random selection of a new value for a given note is controlled by a new parameter, Random Selection Rate (RSR), different than the complementary HMCR probability (1-HMCR) used by the nominal HS algorithm.
   - The Pitch Adjusting Rate, PAR $\in [0,1]$, which sets the probability that the new note value is picked from its neighbor value in the symbol/delay alphabet.

C. The quality **evaluation** and the harmony memory **update** is made at each iteration based on the fitness function in expression (4). At each iteration φ new candidate harmonies (symbols and delays) are improvised and evaluated, but will be included in the harmony memory only if they improve the quality (fitness) of the φ harmonies remaining from the previous iteration.

D. The proposed scheme includes a **perturbing** criterium when all harmonies of any of the two harmony memories (either symbols or delays) becomes uniform, i.e. populated with the same harmony. In this case, as a means to increase the diversity of the algorithm, the perturbing criterium changes randomly the value of a fixed number of notes (denoted as ϱ) in the $\varphi - 1$ worse harmonies of the uniform harmony memory. The best candidate in the given memory is kept unmodified. The resulting harmonies are always accepted disregarding the quality of their fitness.

E. The algorithm stops the iterative process when 1) the metric of the best harmony falls below a certain threshold which, in the simulations presented in this paper, is set to a multiplicative factor κ of the noise standard deviation σ; or 2) a fixed number of iterations $\mathcal{I}$ is reached. The selected stop criterium is an important task for the tradeoff between computational complexity and error performance of the algorithm. If the stop criterium is not satisfied, the algorithm continues the iterative process from point B.

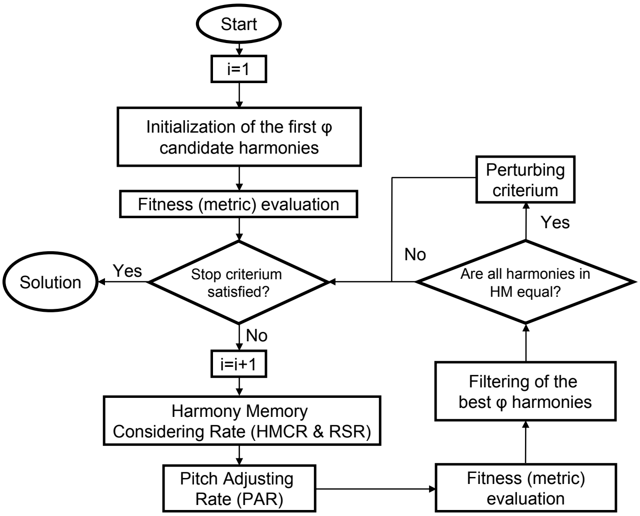

Start
i=1
Initialization of the first φ candidate harmonies
Fitness (metric) evaluation
Stop criterium satisfied?
Yes
Solution
No
i=i+1
Harmony Memory Considering Rate (HMCR & RSR)
Pitch Adjusting Rate (PAR)
Fitness (metric) evaluation
Filtering of the best φ harmonies
Are all harmonies in HM equal?
Yes
Perturbing criterium
No

Fig. 2. Flow diagram of the proposed CDMA MUD detector (i denotes iteration)

When comparing the Harmony Search with the classical Genetic Algorithm, essential differences arise mainly based on the improvisation process for the new harmonies. In the case of genetic algorithms, new genes for a chromosome are obtained from the genes of two parents. In the case of Harmony Memory, however, new values for notes are taken from the value of this note in all the other harmonies included in the harmony memory. Intuitively, from this observation one infers that HS is a more *explorative* heuristic optimization algorithm when compared to the more *exploitative* genetically-inspired search.

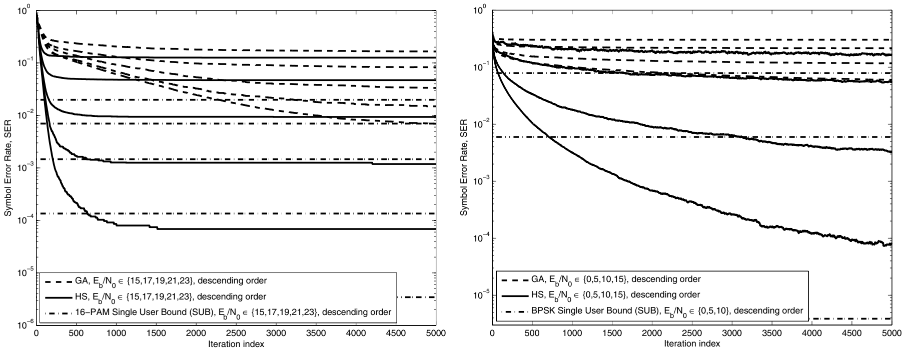
4 Simulation Results

In order to assess the performance of the proposed detector, intensive computer simulations have been carried out by comparing the convergence of both HS- and GA-based MUD detectors in two different scenarios, as described in the following:

- The first scenario consists of $N = 7$ fully-synchronous CDMA transmitters transmitting 16-PAM modulated data to a central receiver. The spreading sequences are pseudo-randomly generated at the beginning of the Monte Carlo simulation, with a spreading factor of $L = 12$ chips. The parameters of the proposed HS-based detector are set to $(\mathrm{HMCR}, \mathrm{RSR}, \mathrm{PAR}) = (0.9, 0.1, 0.1)$, and the size of the harmony memory is equal to $\vartheta = 16$. For the GA-based detector, a population of 16 *chromosomes* with an elite pool size of 8 individuals has been used, whereas the selection process is based on the Roulette-Wheel criterium [22] with an uniform crossover rate [23] of $P_c = 0.9$ and a mutation probability of $P_m = 0.3$. It should be noted that the choice of the values for all parameters has been done after intensive simulation-based optimization studies. Also note that in this scenario the complexity of an ML detector based on exhaustive search would be $M^N = 268,435,456$ metric evaluations.
- The second scenario is composed of $N = 5$ quasi-asynchronous nodes transmitting BPSK ($M = 2$) modulated data to the common destination, with L kept fixed to 12, pseudo-randomly generated CDMA codes, and a maximum delay factor $\xi_{\max} = 4$. Therefore, the delays $\{\tau_n\}_{n=1}^{N}$ are randomly and independently drawn from the set $\{0, \ldots, 4T_c\}$ at every symbol period T_s. The parameters of the HS-based MUD detector are given by $(\mathrm{HMCR}, \mathrm{RSR}, \mathrm{PAR}) = (0.99, 0.2, 0.2)$, with again $\vartheta = 16$ candidates in the harmony memory. Regarding the GA-based detector, the sizes of the population and elite pools are set to 16 and 8 individuals and P_c and P_m are equal to 0.7 and 0.3, respectively. The values for these parameters (i.e. HMCR, RSR, PAR, P_m and P_c) are set identical for both symbol and delay harmony memories. In this case, the complexity of the optimum ML detector is $(\xi_{\max})^N \times M^N = 32,768$ metric evaluations.

In both simulated scenarios, the maximum number of iterations of the HS and GA detection algorithms is $\mathcal{I} = 5,000$ and the number of notes affected by the perturbing criterium detailed in Section 3 is given by $\varrho = 5$. The alternate stop criterium based on thresholding the metric by a multiple of the channel noise standard deviation uses $\kappa = \sqrt{N}$, which accounts for the fraction of σ per user. It should also be noted that in all cases, no a priori information on the delays and/or the harmonies is assumed at the receiver.

Having said this, Figure 3.a depicts the Symbol Error Rate (SER) as a function of the iteration index for the first simulated scenario, a range of energy per bit to noise spectral density amplitude $E_b/N_0 \in \{15, 17, 19, 21, 23\}$ (in dB), and both considered heuristic detection algorithms. Also are included in the plot horizontal asymptotes corresponding to the SER values of a point-to-point single-user 16-PAM transmission over an AWGN channel with $E_b/N_0 \in \{15, 17, 19, 21, 23\}$. For the sake of clarity no markers are included in the plot, where it should be read that the curves are drawn in descending order from $E_b/N_0 = 15$ dB (upper set of curves) to $E_b/N_0 = 23$ dB (lower set of curves). Observe that the HS-based MUD detector proposed in this paper not only outperforms the GA-assisted detector significantly in terms of SER, but also converges in much fewer iterations. For instance, when $E_b/N_0 = 17$ dB the HS-based detector converges to $SER \approx 4.8 \cdot 10^{-2}$ in roughly 400 iterations, as opposed to the GA-based approach whose SER reaches $8.5 \cdot 10^{-2}$ at 2,300 iterations. For this E_b/N_0 level, these SER values are attained at an complexity of 13,920 (HS) and 25,200 (GA) average metric evaluations, which are computed as the product of ϑ (equivalently, population size) and the average number of iterations within the corresponding algorithm converges.



(a) (b)

Fig. 3. (a) SER convergence versus iteration index of the two considered heuristic MUD detection techniques for (a) the first simulated scenario (16-PAM, synchronous); (b) the second simulated scenario (BPSK, quasi-synchronous)

Let us now focus on Figure 3.b, where the SER curves corresponding to the second simulated scenario are plotted in a similar arrangement to Figure 3.a. In this case, although the distance to the BPSK single-user SER bound increases for both HS-based and GA-based detection algorithms, the SER performance gap between such techniques augmentates dramatically while maintaining the reduced average computational complexity of the first commented scenario. For instance, at $E_b/N_0 = 15$ dB the HS-based detector requires on average 1,136 metric evaluations, in comparison to the 15,568 average evaluations of the objective function in the GA approach. Future research will be conducted towards narrowing the performance gap to the single-user SER bound of the proposed HS-based detector in this second scenario.

5 Conclusions

In this paper we have proposed a novel heuristic MUD technique for quasi-asynchronous CDMA systems employing multilevel amplitude signalling. The proposed detector is based on the Harmony Search heuristic algorithm, and sequentially iterates between a pool of φ candidate symbol vectors (symbol harmony memory) and φ sets of time delay candidates (delay harmony memory). The progressive refinement of these sets is governed by a set of parameters controlling the convergence behavior of the proposed detector. The presented simulation results state that the HS-based detector here proposed is able to outperform alternate MUD detection approaches based on classical Genetic Algorithms in terms of end-to-end Symbol Error Rate while requiring, at the same time, much less complexity.

Further work on this topic will gravitate around optimizing the perturbing criterium utilized to escape from the local minima, combining the HS-based procedure with concepts drawn from Tabu Search [24,25], and improving the a priori information fed to the detector in order to enhance the starting state of the algorithm. Investigations will be also focused on jointly optimizing the symbol and delay harmonies, as opposed to the sequential approach adopted in this work.

Acknowledgments

This work was supported in part by the Spanish Ministry of Science and Innovation through the CONSOLIDER-INGENIO 2010 (CSD200800010), the Torres-Quevedo (PTQ-09-01-00740, PTQ-06-01-0159) funding programs, as well as by the Basque Government through the ETORTEK Programme (*Future Internet* EI08-227 project).

References

1. Garey, M.R., Johnson, D.S.: Computer and Intractability: A Guide to the Theory of NP-completeness. W. H. Freeman and Company, New York (1979)
2. Chang, C.J., Wu, C.H.: Optimal Frame Pattern Design for a TDMA Mobile Communication System Using a Simulated Annealing Algorithm. IEEE Transactions on Vehicular Technology 42(2), 205–211 (1993)
3. White, M.S., Flockton, S.J.: A Genetic Adaptive Algorithm for Data Equalization. In: Proceedings of the First IEEE Conference on Evolutionary Computation, IEEE World Congress on Computational Intelligence, vol. 2, pp. 665–669 (1994)
4. Chen, S., Wu, Y., McLaughlin, S.: Genetic Algorithm Optimization for Blind Channel Identification with Higher Order Cumulant Fitting. IEEE Transactions on Evolutionary Computation 1(4), 259–265 (1997)
5. Salcedo-Sanz, S., Yao, X.: Assignment of Cells to Switches in a Cellular Mobile Network using a Hybrid Hopfield Network-Genetic Algorithm Approach. Applied Soft Computing 8(1), 216–224 (2008)

6. Salcedo-Sanz, S., Portilla-Figueras, J.A., Garcia-Vazquez, F., Jimenez-Fernandez, S.: Solving Terminal Assignment Problems with Groups Encoding: The Wedding Banquet Problem. Engineering Applications of Artificial Intelligence 19, 569–578 (2006)
7. Alonso-Garrido, O., Salcedo-Sanz, S., Agustin-Blas, L.E., Ortiz-Garcia, E.G., Perez-Bellido, A.M., Portilla-Figueras, J.A.: A Hybrid Grouping Genetic Algorithm for the Multiple-Type Access Node Location Problem. In: Corchado, E., Yin, H. (eds.) IDEAL 2009. LNCS, vol. 5788, pp. 376–383. Springer, Heidelberg (2009)
8. Landa, I., Garcia-Padrones, L., Gil-Lopez, S., Del Ser, J., Salcedo-Sanz, S.: On the Application of a Novel Grouping Harmony Search Algorithm to the Heterogeneous Access Node Location Problem. Submitted to 2nd International Conference on Mobile Lightweight Systems (MOBILIGHT), Barcelona, Spain (2009)
9. Verdu, S.: Minimum probability of Error for Asynchronous Gaussian Multiple Access Channel. IEEE Transaction of Information Theory 32, 85–96 (1986)
10. Juntti, M.J., Schlosser, T., Lilleberg, J.O.: Genetic Algorithms for Multiuser Detection in Synchronous CDMA. In: IEEE International Symposium on Information Theory, Ulm, Germany, p. 492 (1997)
11. Jiang, M., Akhtman, J., Hanzo, L.: Genetic Algorithm Joint Channel Estimation and MUD for SDMA OFDM. OFDM and MC-CDMA: A Primer, pp. 303–330. John Wiley, Chichester (2006)
12. Ciriaco, F., Abrao, T., Jeszensky, P.J.E.: DS-CDMA Multiuser Detection with Evolutionary Algorithms. Journal of Universal Computer Science 12(4), 450–480 (2006)
13. Naeem, M., Ismail, S.S., Jamal, H.: Multiuser Detection in CDMA Fast Fading Multipath Channel using Heuristic Genetic Algorithms. World Academy of Science Engineering and Technology 12, 19–23 (2005)
14. Yen, K., Hanzo, L.: Genetic-Assisted Joint Multiuser Symbol Detection and Fading Channel Estimation for Synchronous CDMA Systems. IEEE Journal on Selected Areas in Communications 19(6), 985–998 (2001)
15. Geem, Z.W., Hoon Kim, J., Loganathan, G.V.: A New Heuristic Optimization Algorithm: Harmony Search. Simulation 76(2), 60–68 (2001)
16. Geem, Z.W.: Optimal Cost Design of Water Distribution Networks using Harmony Search. Engineering Optimization 38(3), 259–277 (2006)
17. Forsati, R., Haghighat, A.T., Mahdavi, M.: Harmony Search Based Algorithms for Bandwidth-Delay-Constrained Least-Cost Multicast Routing. Computer Communications 31(10), 2505–2519 (2008)
18. Geem, Z.W.: Harmony Search Algorithm for Solving Sudoku. In: Apolloni, B., Howlett, R.J., Jain, L. (eds.) KES 2007, Part I. LNCS (LNAI), vol. 4692, pp. 371–378. Springer, Heidelberg (2007)
19. Gil-Lopez, S., Del Ser, J., Olabarrieta, I.: A Novel Heuristic Algorithm for MultiUser Detection in Synchronous CDMA Wireless Sensor Networks. In: IEEE International Conference on Ultra Modern Telecommunications, San Petersburgo, Russia (2009)
20. Zhang, R., Hanzo, L.: Iterative Detection and Channel Decoding for DS-CDMA Using Harmony Search. IEEE Signal Processing Letters 16(10), 917–920 (2009)
21. Ng, S.X., Yen, K., Hanzo, L.: M-ary Coded Modulation Assisted Genetic Algorithm Based Multiuser Detection for CDMA Systems. In: IEEE Wireless Communications and Networking Conference, vol. 2, pp. 779–783 (2003)

22. Goldberg, D.E.: Genetic Algorithms in Search, Optimization, and Machine Learning. Adison-Wesley, Reading (1989)
23. Syswerda, G.: Uniform Crossover in Genetic Algorithms. In: Third International Conference in Genetic Algorithms, pp. 2–9 (1989)
24. Glober, F.: Tabu Search–Part I. ORSA Journal on Computing 1(3), 190–206 (1989)
25. Glober, F.: Tabu Search–Part II. ORSA Journal on Computing 2(1), 4–32 (1989)

Cross-Layer Clustering Optimization in Mobile Networks Using Evolutionary Algorithms

L. Carro-Calvo, S. Maldonado-Bascon, A. Portilla-Figueras,
S. Lafuente-Arroyo, and S. Salcedo-Sanz

Universidad de Alcalá, Spain
sancho.salcedo@uah.es

Abstract. In this paper we present an evolutionary algorithm to tackle the aggregation network design in a mobile communication system. The design and optimization of this part of the network involves four different tasks: the determination of the number and location of the Base Station Controller (BSC) or Radio Network Controllers (RNC), the assignment of Base Stations (BTS) or B-Nodes to the controllers, the definition of the tree structure that links all the nodes with the controllers and, finally, the system assignment in the links between the different hops of the tree. The novel evolutionary heuristic proposed deals with all these sub-problem together and it is able to obtain good solutions, as will be shown in several real scenarios.

Keywords: Aggregation network, multi-layer optimization, evolutionary algorithms.

1 Introduction

Traditionally, the main problem in the design of mobile telecommunication networks is related to the cell deployment [2], i.e., to the definition of the type, number and location of BTSs in 2G systems, or B-Nodes in 3G ones, that are required to provide coverage to a specific area.

The aggregation network (transport network between the terminal nodes, the BTS and the BSC) design has been considered sometimes a low relevancy task, implemented by leased lines of a fixed operator. However as the data services have become popular, and the required bandwidth upstream the BSC has increased, the design of this part of the network has gained higher relevance again, becoming one of the main problems in the access network planning.

The design of the aggregation network involves three different tasks:

1. Logical layer design: It consists on the cluster definition, i.e., the determination of the number and location of the Base Station Controller and the definition of which BTS are assigned to each BSC.
2. Physical layer design: For each of the clusters defined in the logical layer, the physical topology that links all BTS with the BSC is determined, usually forming a tree structure. Note that some new network elements, as Hubs to

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 638–649, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

concentrate links up-streams or link repeaters (with no logical function) has to be considered in this task.

3. System Assignment: Once the previous tasks have been carried out, this task calculates the type and number of network equipments (ports, link systems, etc.) to provide enough capacity to the network previously designed.

Traditionally aggregation network optimization has been tackled trying to optimize each task separately. The Logical layer design could be considered as a terminal assignment problem with capacity restrictions, [3]. Intense research has been carried out in field, using different approaches, from traditional ones, see [4], to evolutionary or hybrid meta-heuristics, [6], [5]. The same situation could be observed in the physical layer design. There are quite broad literature about tree topology design with capacity, distance and reliability restrictions [7], [8]. Finally, when the network is completely designed, the system assignment is just a deterministic procedure using the most suitable equipment for each network element [9].

Although these studies offer interesting results in terms of network investment cost, the problem of network optimization has to be considered under a global perspective. Note that small changes in the clustering procedure obtained in the aggregation network design may produce dramatic changes in the network topology, which may result in important cost reductions. This means that the optimization of the whole aggregation network has to use global procedures under a multi-layer approach. As far as we know, there are not specific works over this point in the literature.

This paper proposes a novel heuristic to tackle the multi-layer optimization problem in the aggregation part of a mobile network. The proposed heuristic is based on an evolutionary algorithm that optimizes the investment cost of the calculated network. This is done by considering traffic and physical ports capacity constraints in the links and nodes, and also distance restrictions in the links.

The rest of the paper is organized as follows. Next section provides a mathematical description of the problem. Section 3 presents in detail the proposed evolutionary algorithm. Section 4 provides a description of the experiments carried out to test the performance of the proposed algorithm. Finally the conclusions section discusses the applicability of the proposed heuristic and some future work lines.

2 Problem Definition

Let us consider a set of N BTSs from $n = 1, \ldots, N$ and a set of M BSCs from $m = 1, \ldots, M$. Each BTS n handles a traffic of A_n Erlangs, which has to be routed from the BTS up to the BSC where it is assigned. Each BSC m has a maximum capacity in terms of traffic Ca, and also in the number of radio links that could be physically connected to it, Crl.

We consider that, as usually, the logical connections between the BTSs and the BSCs are done considering a star structure, where all the BTSs are directly linked to the BSC. On the other hand, the physical communication between the

BTSs and the BSC is done using a tree-structured network. Each branch of the tree is connected to the main trunk by a BTS-hub which concentrates the traffic of the BTSs that are under it in the branch. To save costs, the BTS-hub is placed in the same location as an existing BTS. The BTS-hub has a limited capacity, defined by Crl_{hub}, involving the number of radio links of the BTSs that could be connected to it.

The connections between network elements, BTS-hubs, BTS-BSC or hub-BSC, are implemented by radio links RL. The maximum distance each radio link can reach is defined by d_{RL} and the traffic flow as A_{RL}. Each radio link implements a specific transmission system TS_i from a set of systems $i = 1, \ldots, I$ which has a maximum capacity in terms of the traffic it can handle, C_i and an associated cost Q_i. Furthermore, the reliability of each radio link decreases as a function of the radio link length RL_d, let us name it $f(RL_d)$.

Each network element has a corresponding associated cost. The cost of the BSC and the hub are Q^{BSC} and Q^{Hub} respectively. For each radio link, there are three different costs. The first one is associated with the required physical port to implement in the hub or in the BSC, Q^{port}. The second cost depends on the type of system that has to be implemented to carry the traffic of the BTSs in the branch of the tree. Systems which support higher capacity will have higher costs Q^S. Finally if we need to link two network elements separated more than d_{RL} an additional repeater equipment will be required, and hence we will have to add the corresponding Q^R.

To find the complete network configuration we have identified the following two subproblems:

2.1 First Sub-problem: Capacitated Clustering Problem

The first subproblem consists of the logical assignment of BTSs to BSCs, to define the M clusters of the network, see Figure 1 (a). Each BTS is assigned to its nearest BSC with enough free capacity. This is a classical terminal assignment problem with capacity limits in the concentrator node. The fitness function tries to minimize the total aggregated distances. Let us consider that K_m, $m = 1 \cdots M$, is the set of BTSs assigned to the BSC m. Let us also consider that d_n^{BTS} is the distance between the BTS n and its corresponding BSC. Therefore the objective function may be defined as follows.

$$\min \left(\sum_{i=1}^{N} d_i^{BTS} \right) \tag{1}$$

Subject to:

$$\sum_{\forall\ BTS\ \in\ K_m} A_n \leq Ca, \forall K_m,\ m = \{1, \ldots, M\}. \tag{2}$$

2.2 Second Sub-problem: Tree Structured Physical Topology

The second subproblem consists in the definition of the tree structure between the BSC and the BTSs associated to it, see Figure 1 (b). To do this, we need to determine the location of each hub h, $h = 1 \cdots H$ in the cluster K_m and the physical links between the BTSs and hubs or BSCs. Note that the value of H changes for each cluster. Furthermore, we need to calculate the aggregated traffic flow from the BTSs upstream to the BSC in order to determine the type of transmission system that has to be implemented. There are also some constrains related to the capacity of the BSC, Crl, the maximum capacity of the hub, Crl_{hub}, the maximum length and reliability of the radio links, d_{RL} and $f(RL_d)$ and the maximum capacity of the transmission system C_i. The objective is to minimize the total cost of the tree topology of each cluster K_m, Q_{K_m} following the equation:

$$\min\left(Q_{K_m}\right) = Q^{BSC} + Q^{Links} + NHubs_{K_m} \cdot Q^{Hub}, \tag{3}$$

where $NHubs_{K_m}$ is the number of hubs required in the BSC cluster K_m and Q_{Links} is the total cost of all radio links RL in the BSC cluster given by the following:

$$Q_{Links} = \sum_{\forall RL \in K_m} Q^{Port} + Q_i + N_{Repeaters}\left(Q^R + Q_i\right) \tag{4}$$

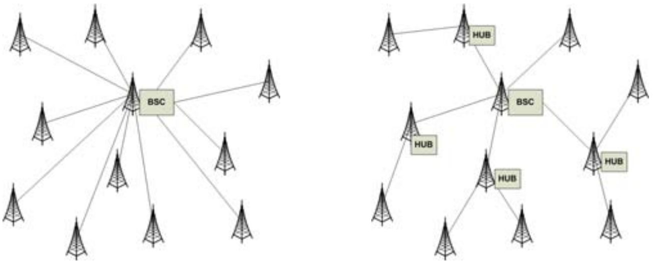
The constraints for this tree structure are:

$$|RL_{BSC} \in K_m| \leq Crl \tag{5}$$

$$|RL_{Hub}| \leq Crl_{hub}\, \forall Hub \in K_m \tag{6}$$

$$A_{RL} \in K_m \leq Ca_i\, \forall RL \in K_m \tag{7}$$

$$\min_{\forall \text{Branchs} \in K_m}\left(\prod_{\forall \text{links in Branch}} f(RL_d)\right) \geq f_{min} \tag{8}$$



(a) (b)

Fig. 1. Problem definition; (a) Logical layer (star structure topology); (b) Physical layer (tree structure topology)

Equation (5) specifies that the number of radio-links connected to the BSC do not exceed the capacity of the BSC. Equation (6) applies the same criteria for the hubs in the cluster. Equation 7 assures that the capacity of the transmission system implemented in each radio-link RL is enough to carry the traffic flow of the link. Finally, Equation (8) defines the requirements in terms of reliability. It analyzes the less reliable branch in the three and compares it with a minimum threshold defined by f_{min}.

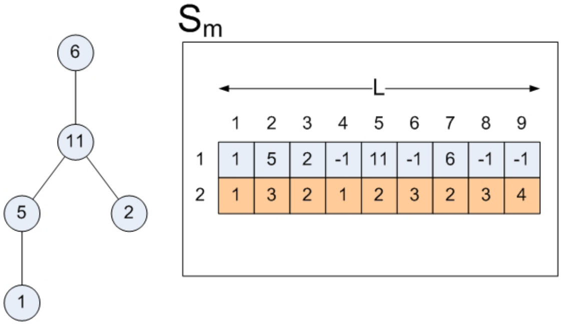
3 Proposed Evolutionary Algorithm

This section presents the proposed meta-heuristic algorithm to solve this problem. Specifically, it is an evolutionary algorithm adapted to tackle with the different sub-problems of the aggregation network optimization problem tackled. This section is divided into three subsections: the first one deals with the solutions encoding into the algorithm, the second one explains the initialization of the algorithm and the fitness function used, and finally the third one shows the evolutionary operators used.

3.1 Solution Encoding

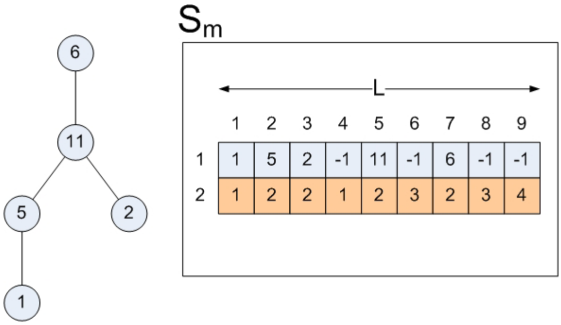
The complete network is composed of M clusters corresponding to the M BSCs of the problems. Therefore the physical structure will be composed of M trees. Let L be the maximum possible number of BTSs that can be allocated in a single cluster. Note that L will be chosen as a value that ensures a feasible encoding of our algorithm. Then, each tree is codified in the evolutionary algorithm as an integer $2 \times L$ matrix S_m (note that an individual in the evolutionary algorithm is formed by M matrices S_m). The coding of the tree is done from the leafs to the trunk, what means that the lower level BTSs are on the leftmost positions of the matrix. Each position of the first row of the matrix stores either a BTS identifier, $i = 1 \dots K_m$, or the value -1. The second row stores the jump to the position in the matrix where the preceding BTS in the tree is located. Let us illustrate this encoding method with a graphical example. Consider a single cluster with nodes $n = \{1, 5, 2, 11, 6\}$ in it, in hierarchical order from leafs to trunk. The maximum number of nodes per cluster is $L = 9$. Figure 2 shows the corresponding matrix encoding and the resulting decoded tree. Note that node 1 of the cluster m in position $S_m(1, 1)$ of the matrix is linked to node 5 in the tree. Then, the value in position $S_m(2, 1)$ of the matrix is 1 which is the jump to the position of the node 5 in the matrix. The same happens with node 5 and node 11. The value in the position $S_m(2, 2)$ is 3, the jump to the position of node 11 in the matrix.

As we are using an evolutionary algorithm, to encourage the diversity of the search space we also allow jumps to non-feasible positions in the matrix. In this case, the tree decoding will use the next feasible position where a BTS is stored. Thus, Figure 3 shows a different encoding for the previous example which is also valid. In this case, the jump in position $S_m(2, 2)$ indicates a position in the



	1	2	3	4	5	6	7	8	9
1	1	5	2	-1	11	-1	6	-1	-1
2	1	3	2	1	2	3	2	3	4

Fig. 2. Example of tree structure encoding



	1	2	3	4	5	6	7	8	9
1	1	5	2	-1	11	-1	6	-1	-1
2	1	2	2	1	2	3	2	3	4

Fig. 3. Example of tree structure encoding with jumps to non-valid positions

matrix with no BTS, denoted by a -1. Therefore, the decoding of the tree will look for the next feasible position, which is again the position corresponding to node 11. In both cases, when the decoding algorithm reaches to the root node (BSC of the cluster, in the example node number 6), no further jumps are allowed in the matrix.

3.2 Initialization

The proposed heuristic will determine the optimum clustering distribution by means of crossover and mutation procedures that will be explained in subsection 3.7. However for the algorithm initialization we will use a $p-median$ algorithm which is described in [5].

The $p-median$ algorithm provides from the complete set of nodes of the experiment the division in the M clusters with the corresponding M BSC or root nodes. This algorithm minimizes the total distance between the nodes in the cluster under the capacity constraint of the BSC. The tree structure of each cluster defined by the $p-median$ algorithm is randomly generated, $S_m(1,j)$ for $i = 1 \ldots L$. Note that although the $p-median$ algorithm defines a root node (the BSC) for each cluster, our algorithm does not consider them to proceed to a further optimization of the total network structure.

The second row of the matrix S_m, which represents the jumps in the tree structures, is initialized as follows: each position $S_m(2, j)$, $j = 1, \ldots, L$ takes a value that is randomly generated following a uniform distribution in the interval $[1, p]$. Parameter p models the initial topology of the cluster. If $p \approx 1$ the cluster structure will tend to form a chain. Opposite if $p \approx L$ the structure of the cluster will tend to be a star. Therefore we have fixed the value of p to $L/2$.

3.3 Reliability of the Branches

An important point in this implementation is the reliability of the links. We consider that each link has a reliability of $f_{RL} = 0.994$ that could be considered constant in the distance range $[0, d_{RL}]$. The reliability is calculated from the leaves to the root of the tree. Each node in the branch has a reliability value, f_{node} that is the minimum over of the reliability values of all branches under it. The value of the reliability of each branch is calculated multiplying the current reliability value, by the value of the next link upstream in the tree. When the current value of the reliability in a node is lower than a minimum threshold f_{min} we consider a penalty value P_f that is linearly incremented depending on the number of nodes upstream the current one. Of course this solution will not be feasible and hence will be surely discarded by the evolutionary algorithm. This procedure is graphically explained in Figure 4.

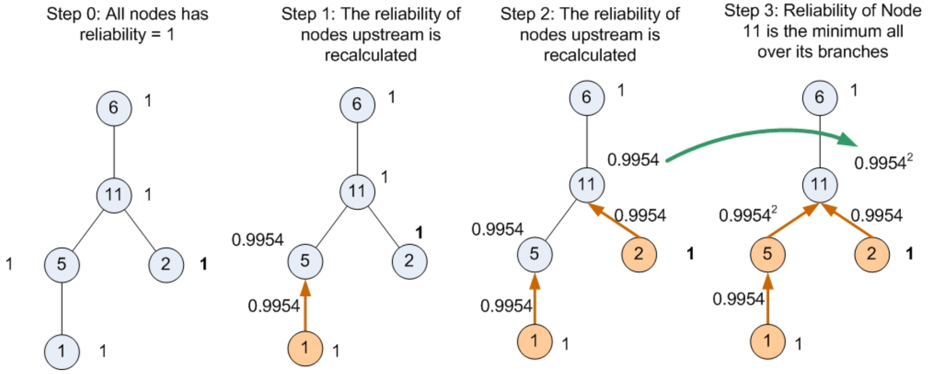

Step 0: All nodes has reliability = 1
Step 1: The reliability of nodes upstream is recalculated
Step 2: The reliability of nodes upstream is recalculated
Step 3: Reliability of Node 11 is the minimum all over its branches
6
11
5
2
1
0.9954
0.9954²
1

Fig. 4. Example reliability calculation procedure

3.4 Capacity of the Hubs and BSC

In Section 2.2 we have considered the capacity constraints of the hubs and BSC related to the number of physical interfaces. The solution obtained by the evolutionary algorithm will not be feasible if these capacities are exceeded. Therefore, we introduce a penalty factor P_p in the fitness function that linearly depends on the exceeding ports in the hubs and BSC of the current solution. Regarding the BSC, there is an additional constraint related with the traffic capacity. This constraint is related to the logical capacity of the BSC and it could not be applied to the hubs. The maximum traffic handled by the BSC has to be lower than a maximum value Ca. If this value is overcome, the solution is again unfeasible, and the corresponding penalty, P_c has to be applied in the fitness function.

3.5 Large Distance Penalties

Early experiments performed with the algorithm showed that in some cases, there were some crossed links in the clusters. To solve this point and to reduce the length of the cluster links (hence to minimize the cost function), we have introduced a penalty for large distance links, P_d. The value of this penalty is obtained from a stepwise function, where each step has a different slope as it is shown in Figure 5.

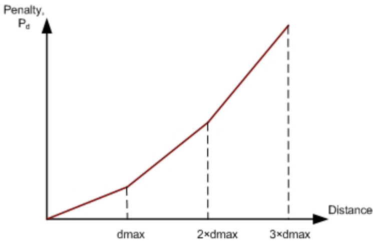


Fig. 5. Example of stepwise distance penalty function with different slopes

3.6 Fitness Function

The proposed evolutionary algorithm uses a fitness function closely related to the one shown in Equation (3). Note that the proposed algorithm performs a multi-layer optimization. This means that we try to simultaneously optimize, the cluster organization in the logical layer (see subsection 3.7), the cluster topology in the physical layer and finally the system assignment. A very difficult problem when tackling this multi-layer problem is to calculate the traffic flow upstream in the tree, because it depends on the physical topology. To overcome this difficulty, our fitness function is calculated at the same time that the trees are being decoded. To do this, we define a new vector O_m, with length L, that stores, for each node in the current tree, the number of radio links downstream to the next level in the tree. We also define a cost $Qagg_m$ which represents the aggregated cost of the network elements and systems that is calculated as we climb the tree towards the root node.

Summarizing, the final cost of the cluster Q_{K_m} is:

$$Q_{K_m} = Qagg_m + \alpha \cdot P_f + \beta \cdot P_c + \delta \cdot P_p + \eta \cdot P_d \tag{9}$$

And the value of the fitness function of each individual

$$\sum_{\forall K_m} Q_{K_m} \tag{10}$$

3.7 Evolutionary Operators

Selection operator. Once we have calculated the fitness value for each individual, the algorithm calculates the average value of all individuals. All those individuals with a fitness value above the average are discarded. Note that the algorithm tries to optimize the total cost of the network so lower values of the fitness function, that is lower cost, are better than higher values. Each discarded individual is replaced by a new individual resulting from the crossover and mutation operators, applied over the reduced population, that are explained below.

Crossover Operator. The crossover operator implemented in our evolutionary algorithm considers only intra-cluster changes. From the complete set of individuals, we randomly select two of them to be the parents of one individual in the next generation. Remember that each individual is a set of M trees, where each cluster is codified using the matrix S_m. Each position in the matrix of the new individual, for example $S_m(1,5)$ and $S_m(2,5)$ is randomly selected from the equivalent positions $S_m(1,5)$ and $S_m(2,5)$ in the parent matrix with probability 0.5. The crossover procedure has a list of all nodes that have been added to the new individual, so it guarantees that nodes previously added to the new individual are not available for following assignment.

At the end of this procedure, there could be some nodes that are not assigned to any cluster in the new individual. To repair this solution, these nodes are included in the first free position of the same cluster they were in the first parent. To guarantee the coherency, in the second line of the cluster matrix, S_m, the value of the jump is modified to point to the same position as in the first parent. If the node is after that position, the value of the jump is fixed to 1.

Mutation operator. The proposed heuristic uses three type of mutations, two of them act inside the same cluster and the third one induces changes between two different clusters. The first intra-cluster mutation swaps two randomly selected nodes in the structure of the tree. This mutation is applied to 1/8 of the total number of nodes with probability 0.1.

The second intra-cluster mutation modifies the value of the jump in the second line of the matrix S_m of a randomly selected node of $M/10$ randomly selected clusters. The value of the jump of this randomly selected node is fixed to 1 with probability 1/5. This means an enlargement of the tree because this node will be now connected to a node closer to the leafs. With probability 4/5 the jump will take the value required to be linked to the node above its current parent node. This means a shortening of the tree.

The last mutation operator performs a swap between nodes from different clusters, randomly selected. Note that only the node identifier j in the first row of matrix $S_m(1, j)$ is swapped in order to keep the mathematical structure of the tree. To avoid dramatic changes in the geographical structure of the tree, the swapping probability is higher for the nodes of the surrounding clusters.

4 Experiments and Results

To test the performance of the algorithm we have developed a set of three experimental examples. Each one is composed of a subset of the most important districts in Spain. The complete scenario consists of 881 districts, with a population greater of equal to 1000 inhabitants. This information has been obtained from the Spanish National Statistic Institute. For the experiments we consider the case of an mobile operator with 25% of market share. The Spanish penetration of the mobile service is 110% on average. We consider that a single BTS provides service to 5200 inhabitants following the results in [1]. The individual traffic per user is 12.5 mErlangs as it results from [10]. Using the Erlang B formulation, and considering 16Kbps circuits in the Abis interface [11] between the BTS and the BSC, the total throughput of the district is calculated. We consider that all BTS's links in the district are multiplexed into a single one that is offered to the network structure.

Table 4 shows the main parameters of the experiments carried out. Note that the ratio between the number of BTSs and the number of predefined clusters is 128, that is a typical capacity of a BSC. The cost and capacities of each network equipment is shown in Table 4.

Table 1. Experiments definition

Experiment	Number of Nodes	Total Number of BTS	Number of Clusters
Exp1	300	14190	111
Exp2	600	17134	134
Exp3	881	18131	142

Note that as we have not found any similar work in the literature for comparing with, so a lower bound obtained by considering no capacity constraints neither in the BSC nor in the Hubs is used to validate our approach. We have run each experiment 10 times and we offer the values of the best and average solution and the standard deviation. These results are shown in Table 4. Note that even for the largest experiment, Exp3, the final cost of the best solution obtained is quite close to the lower bound, only 3% higher.

The purpose of this algorithm is to be used as a planning tool in real applications on mobile communications regulatory processes. Therefore an important

Table 2. Cost of the network elements in k€

Element	Cost
Increment BTS/Hub (Q^{Hub})	42.0
HUB card (Q^{port})	2.5
Repeater (Q^R)	21.6
2Mb system (Q^i)	15.0
8Mb system (Q^i)	25.0
34Mb system (Q^i)	38.0
140Mb system (Q^i)	47.0

Table 3. Experimental results

Experiment	Min Cost	Avg Cost	Std. Desv	Lower Bound
Exp1	5177.1	5261.3	17.0 (0.32%)	5081.93
Exp2	11872.0	12105.0	87.0 (0.71%)	11696.12
Exp3	45991.0	47132.0	381.0 (0.80%)	44453.80

feature is the computation time. A large processing time means that the repetition of each experiment becomes a hard task, so it is important to observe the evolution of the algorithm versus time (wall clock time is used in this case). In the experiments carried out, the stopping condition of the evolutionary algorithm was fixed using computation time, with a maximum of 5 minutes of computation (wall clock time). Table 4 shows this evolution. Note that the value of the investment cost obtained at time=1 min is less than 3% worse than the solution obtained at time=4 min even in the Exp3. This error percentage falls inside the tolerance margin of any possible real implementation, so the solution at time=3 min could be a good compromise. The final best solution is obtained at time=5 min.

Table 4. Computational time of the proposed algorithm

Experiment	1 min	2 min	3 min	4 min	5 min (max time)
Exp1	5202.37	5188.72 (-0.26%)	5188.56 (-0.26%)	5095.06 (-2.06%)	5081.93
Exp2	12034.5	11909.3 (-1.04%)	11837.3 (-1.63%)	11759.8 (-2.28%)	11696.12
Exp3	47094.7	46705.8 (-0.82%)	46524.7 (-1.21%)	45497.1 (-1.26%)	44453.80

5 Conclusions

In this paper we have proposed a novel evolutionary heuristic for the multi-layer optimization problem in tree topology access networks. The proposed approach has some innovative characteristics such as the possibility of moving nodes between different clusters, changing the location of the BSC inside each cluster and the form of encoding the tree topology of the clusters. We have run several experiments with increasing number of nodes, from 300 to 881 and the results are very close to a lower bound introduced for the problem. Another key point is the processing time, obtaining good results within short times, about 180 seconds. This makes this algorithm an interesting tool to be used in network planning tasks. In fact the final objective of this work is to substitute the old access network planning algorithms used in previous regulation projects as [1] by the one proposed in order to obtain much more optimized structures.

References

1. Brinkmann, M., Hackbarth, K., Ilic, D., Neu, W., Neumman, K.H., Portilla-Figueras, A.: Mobile Termination Cost Model for Australia. Final Report, `http://www.accc.gov.au`
2. Krishnamachari, B., Wicker, S.: Base station location optimization in cellular wireless networks using heuristic search algorithms. Soft Computing in Communications, 201–219 (2003)
3. Quintero, A., Pierre, S.: Assigning cells to switches in cellular mobile networks: a comparative study. Computer Communications 26, 950–960 (2003)
4. Riis, M.: Deployment of mobile switching centers in a telecommunications network: a stochastic approach. Telecommunication Systems 26(1), 93–109 (2004)
5. Salcedo-Sanz, S., Portilla-Figueras, J.A., Ortiz-Garcia, E.G., Pérez-Bellido, A.M., Thraves, C., Fernández-Anta, A., Yao, X.: Optimal switch location in mobile communication networks using hybrid genetic algorithms. Applied Soft Computing 8, 1486–1497 (2008)
6. Pierre, S., Houeto, F.: Assigning cells to switches in cellular mobile networks using taboo search. IEEE Trans. Syst. Man. Cyber. 32, 351–357 (2002)
7. Lee, Y.J., Atiquzzaman, M.: Exact algorithm for delay-constrained capacitated minimum spanning tree network. IET Communications 1(6), 1238–1247
8. Charnsripinyo, C., Wattanapongsakorn, N.: A Model for Reliable Wireless Access Network Topology Design. Proceedings of the IEEE TENCON 2, 561–564 (2004)
9. Cox, L.A., Sanchez, J.: Designing Least-Cost Survibale Wireless Backhaul Networks. Journal of Heuristics 6(4), 525–540 (2000)
10. Comisión del Mercado de las Telecomunicaciones (Spanish Telecommunication National Regulator), Informe Anual (2008), `http://www.cmt.es`
11. Boucher, N.J.: The cellular radio handbook. J. Willey & Sons, England (2001)

A Case Study of Parameter Control in a Genetic Algorithm: Computer Network Performance

J.A. Fernández-Prieto[1], J. Canada-Bago[1], M.A. Gadeo-Martos[1],
and Juan R. Velasco[2]

[1] Telecommunication Engineering Department, E.P.S. Linares, University of Jaén,
Alfonso X El Sabio, 28, 23700 Linares (Jaén)
{jan,jcbago,gadeo}@ujaen.es
[2] Departament of Automatic, University of Alcalá, Campus Universitario,
28871 Alcala de Henares (Madrid)
juanra@aut.uah.es

Abstract. Genetic Algorithms use different parameters to control their evolutionary search for the solution to problems. However, there are no standard rules for choosing the best parameter values, being difficult to know whether the parameter values must be fixed during a run or must be modified dynamically. Besides, there are many theoretical results on parameter control, but however, very often real world problems call for shortcuts and/or some *ad hoc* solutions. This paper presents an effective approach for optimization of control parameters which is based on a meta-GA combined with an adaptation strategy to improve the GA performance. In order to validate the approach, it has been applied to verify the performance of a real system: a computer network. The results have been compared with the ones obtained for other methods: using fixed and adapted parameter values. A statistical analysis has been done to ascertain whether differences are significant.

Keywords: Parameter control, Computer Networks, Throughput.

1 Introduction

Genetic Algorithms (GAs) are search algorithms based on natural genetics that provide robust search capabilities in complex spaces, and thereby offer a valid approach to problems requiring efficient and effective search processes [1]. The basic idea is to maintain a population of individuals (representing candidate solutions to the problem) that evolves over time through a process of competition.

There are two basic models to implement a GA. The *Generational (or canonical) GA* [1] uses non-overlapping populations so the entire population is replaced by the new generation offspring whilst a S*teady-State GA* [2] operates on overlapping populations in which only a subset of the current population is replaced in each generation. In both cases, the behaviour of the GAs is strongly determined by the balance between exploration (to investigate new and unknown areas in a search space) and exploitation (to make use of knowledge acquired by exploration to reach better positions on the search space) [3]. GAs use a number of parameters to control their evolutionary search for the

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 650–661, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

solution to their given problems. The GA control parameter settings, such as population size, N, probability of crossover, Pc, probability of mutation, Pm, probability of selection, Ps, (to select the individuals from the population in order to use them as parents for the new offspring), are key factors in the determination of the exploitation versus exploration tradeoff. These parameters greatly determine whether the algorithm will find a near-optimum solution, and whether it will find such a solution efficiently. It has long been acknowledged that they have a significant impact on GA performance [4]. However, there are no hard and fast rules for choosing appropriate values for these parameters and many researchers based their choices on tuning the control parameters "by hand", that is, experimenting with different values and selecting the ones that gave the best results (as a problem of trial and error). Later, they reported their results of applying a GA to a particular problem, paraphrasing: ". . . for this experiment, we have used the following parameters: population size of 50, probability of crossover equal to 0.95, etc." without much justification of the choice made [5].

The problem of finding optimal control parameters for GAs has been studied by many authors, from the first until the last recent studies: [3][6][7][8][9][10][11], etc. Michalewicz and Schmidt [11] indicate that there are many theoretical and experimental results on parameter tuning and parameter control, but however, very often real world problems call for shortcuts and/or some *ad hoc* solutions.

According to the *No Free Lunch* theorem [12], an algorithm has different performance on different problems, so an optimal or near-optimal set of control parameters for one GA does not generalize to all cases. This stresses the need for efficient techniques that help finding good parameter settings for a given problem.

Furthermore, different control parameter values may be necessary during the course of a run to induce an optimal exploration/exploitation balance. In [9] the authors argument that any static set of parameters, having the values fixed during a GA run, seems to be inappropriate, and it is desirable to dynamically change parameter values. For instance, large mutation steps can be good in the early generations helping the exploration of the search space while small mutation steps might be needed in the late generations to help fine tuning the optimal individuals. Note that a GA is an intrinsically dynamic, adaptive process. Therefore it is a natural idea to try to modify the control parameter values during the run of the GA. It is possible to do this by using some (possibly heuristic) rules, by taking feedback from the current state of the search, or by employing some self-adaptive mechanism. These changes may affect to a single component of an individual, the whole individual, or even the whole population. Clearly, by changing these values while the algorithm is searching for the solution of the problem, further efficiencies can be gained [13]. For these reasons, Adaptive Genetic Algorithms (AGAs) have been built. They dynamically adjust selected control parameters or genetic operators during the course of evolving a problem solution, offering the most appropriate exploration and exploitation behaviour. The straightforward way to treat this problem is by using parameters that may change over time, that is, by replacing a parameter p by a function p(t), where t is the generation counter. However, if the problem of finding optimal static parameters can be quite difficult, designing an optimal function p(t) may be even more difficult.

However, De Jong [14] indicates that it is a difficult thing to ascertain whether there is any advantage to be gained by dynamically changing the value of a parameter during an GA run and, if so, how to change it. What can we do? Should parameter values be fixed during a run or be modified dynamically? How do changes in a parameter affect the performance of a GA? How does one choose appropriate parameter values?

In this paper we present an approach based on a meta-GA, which is combined with an adaptation strategy of the GA control parameter to find and adjust the optimum parameter values, to improve the GA performance. In order to validate the approach, it has been applied to verify the performance of a real system: a computer network. Different comparisons are performed, aiming to assess the acceptable optimization power of the proposed system. The results have been compared with the ones obtained for other methods: using fixed and adapted parameter values. Moreover, a statistical analysis has been done to ascertain whether differences are significant among the proposed system and the other algorithms.

The remainder of the paper is organized as follows. Section 2 describes a case study, the computer network performance, to illustrate the impact on the GA performance from the control parameter settings and presents the topology of the network exploited in the experiments. Section 3 shows the components of the GA. Section 4 provides the system used to optimize the GA control parameter. Results are reported in Section 5 and finally some conclusions are drawn in Section 6.

2 A Case Study: Computer Network Performance

Nowadays, it is important to test computer networks under realistic traffic loads. Poisson's statistical processes [15] are very often adopted as models of background traffic in order to model the computer network performance. In [16][17], the authors argue that Internet traffic can be well characterized by using Poisson models.

However, other authors [18][19] indicate that the use of Poisson models is a clever choice of background traffic pattern to yield useful results, and the worst/best case analysis cannot be done. Therefore it is necessary a mixed simulation technique based on a GA to explore the solution space. They propose to integrate a GA with a network simulator to drive the generation of critical background traffic. The GA aims at generating the worst-case traffic for the computer network under analysis and finds the traffic configuration that minimizes its performance, given some constraints on the traffic bandwidth. Baldi et al. [18] use the static control parameter values which are shown in Table 1 and Karthik et. al [19] use the shown in Table 2.

However, are these static control parameter values the best to optimize the performance of the GA? Which set of parameter values is better? Why not use an AGA? In this case, how the parameter values must be changed?

Table 1. GA parameter values used in [18]

Parameter	Value
Population size	50
Selection probability	0.4
Crossover probability	1.0
Mutation probability	0.01
Number of generations	500

Table 2. GA parameter values used in [19]

Parameter	Value
Population size	50
Selection probability	0.4
Crossover probability	1.0
Mutation probability	0.005
Number of generations	500

Figure 1 shows the architecture of the environment which integrates the GA and the simulator.

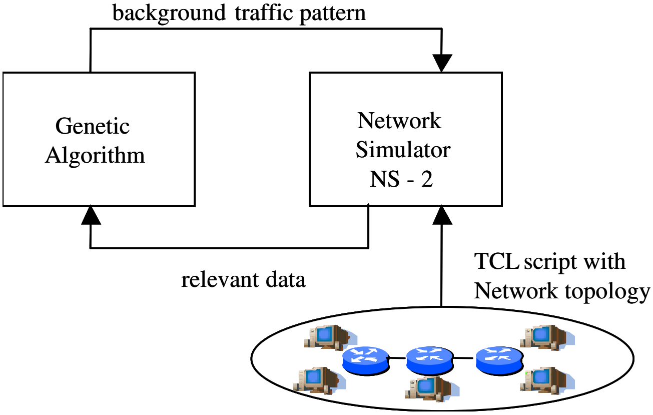


Fig. 1. Architecture of the environment that integrates the GA and the simulator

The approach is quite general and can be applied to different protocols using different simulators with limited effort. We have used a publicly available simulator called ns-2 [20]. It is a discrete event simulator targeted at networking research and provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. The protocol to examine is TCP protocol in order to better focus on the verification methodology and exploitation of the GA and not on the protocol itself. The aim is to study the TCP protocol in real operating conditions. It set up an IP network and a number of TCP probe connections (sender-receiver pairs). The network is loaded with a background traffic generated by UDP (User Datagram Protocol) sender - receiver pairs. During the analysis process, the GA provides a pattern of the traffic generated by background sources and a network simulation is run on the given topology. During this simulation, relevant data are gathered from probe connections by the simulator program and provided to the GA, which uses them to estimate the damage or the benefit that the background traffic made. Such information is then used to drive the generation of traffic patterns to be used in subsequent steps.

2.1 Network Topology

The topology of the network exploited in the experiments is shown in Figure 2. Three TCP connections span from the transmitters TXi to the receivers RXi through three IP routers. Each TCP connection performs long file transfers generating a series of 1024 Kbyte messages at a maximum mean rate of 1.33Mb/s. Acknowledgments from each transmitter are carried by messages flowing in the reverse direction. These TCP connections represent the probe connections of the experiments.

Two sources (BSi) generate background UDP traffic directed to their respective destinations (BDi) over the same links traversed by the TCP connections. The timing of background packets is controlled by the GA. Each link has a capacity of 10Mbps in each direction and introduces a fixed 10μs delay. Routers introduce a fixed 0,1 ms delay component which accounts for the processing required on each packet and adds to the queuing delay.

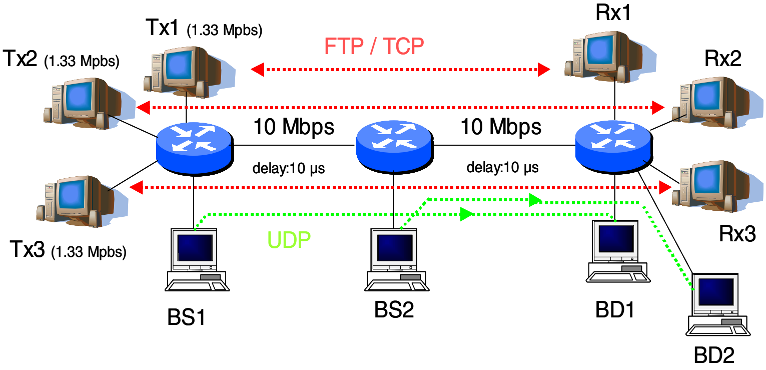


Fig. 2. Topology of the network

3 Genetic Algorithm

For a description of the GA used we have to bear in mind the following five components:

- Solution encoding. Each individual represents a background traffic pattern. Therefore each individual encodes the description of the traffic generated by all the background connections for the whole duration of the simulation. A connection is specified by a UDP source and destination pair. Individuals are encoded as strings of 4500 genes. Each gene represents a single background packet. Genes are composed of the *delay* that represents how long the given source will wait before sending a new packet after sending the current one.
- Initialization. The background traffic corresponding to the initial population is generated according to a Poisson process whose inter-arrival time between packets is exponentially distributed.
- Fitness evaluation. The fitness function measures the probe connections' throughput, i.e., the performance of the probe TCP connections perceived by end users during the simulation experiment. All bytes successfully received at the TCP level, but not delivered to end-users, such as duplicated packets received due to the retransmission mechanism of the protocol, are not considered. The fitness function should increase with the increasing goodness of a solution. As the throughput is being minimized, a solution is good when the background traffic pattern is critical. Therefore, the fitness function is inversely proportional to the total number of bytes perceived by the end users.
- Genetic Operators. The selection operator picks the individuals from the population in order to use them as parents for the new offspring. A selection of individuals of

the population is carried out based on the probability of selection. These individuals are selected according to the tournament selection. The GA applies one point crossover and a random mutation that substitutes each gene with a new random one. After each mutation, genes in the individual need to be sorted. The elitist strategy [6] is considered as well.

- GA parameter values. The parameters used by [18][19] for the GA are summarized in Tables 1 and 2. Instead, we propose to use other probabilities (that may change over time) which have been previously found using our system [21].

Some of the software for the GA used the GAlib genetic algorithm package, which has been written by Matthew Wall at the Massachusetts Institute of Technology [22]. GAlib contains a set of C++ genetic algorithm objects. The library includes tools for using genetic algorithms to do optimization in any C++ program.

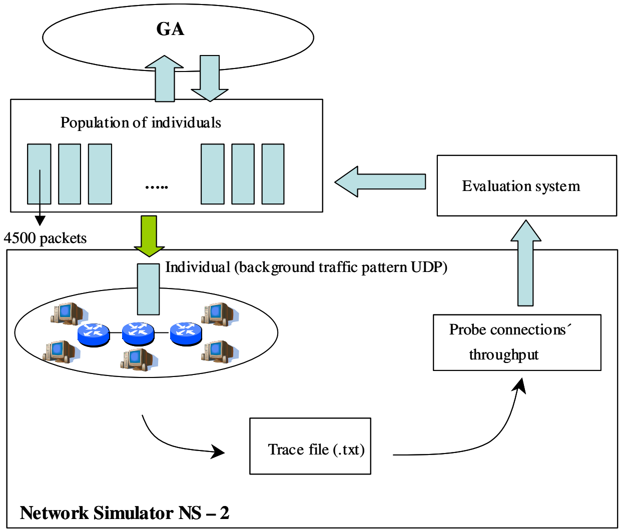

GA
Population of individuals
.....
4500 packets
Evaluation system
Individual (background traffic pattern UDP)
Probe connections´ throughput
Trace file (.txt)
Network Simulator NS – 2

Fig. 3. Genetic Algorithm

4 Optimization of Control Parameters

In order to optimize the control parameters, we propose an approach which is based on a meta-GA (GA within a GA) combined with an adaptation strategy of the GA parameters. The population of the meta-GA consists of a group of GAs, in which each one is running under the same configuration of genetic operators (indicated in Section 3). Each GA can be a Generational GA or Steady-State GA, depending on the selection probability used. The meta-GA is applied to investigate evolving the parameter settings of genetic operators for the GAs.

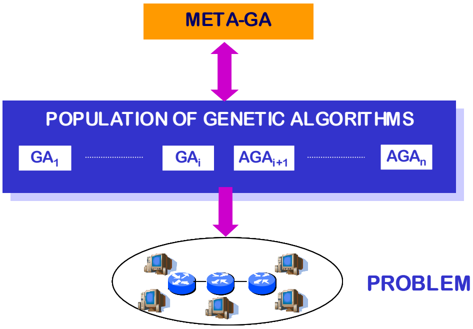


Fig. 4. Approach proposed

However, as indicated in Section 1, the aim of this work is to find the optimum probabilities to improve the GA performance, so really, each individual of the meta-GA population represents a set of probabilities applied to the genetic operators used by each GA. Therefore, we optimize the selection, crossover and mutation probabilities. We do not include the population size in order to establish a reference point to validate the approach. In this way, we can know the GA performance using the parameter values which have been found previously by the meta-AG, and using the parameter values that have been considered frequently in the GA literature [4][6].

The probabilities are dynamically adjusted and can change over time. We use three functions $p_i(t)$, i = 1, 2, 3 where each one affects to Ps, Pc and Pm independently. Each function has the following form:

$$p(t) = p_o^i\left(1 - \frac{(Ln(t+1))^{(1/a_i)}}{(c_i Ln(T+1))^{(1/a_i)}}\right) \qquad \begin{array}{l} a_i \in]0,2] \\ c_i \in [1,\mathrm{T}] \end{array} \tag{1}$$

where p_o^i is the initial value of the probability, t is the generation counter which shall be kept in the interval [0, T] (T is the maximum of generations). The parameter a_i models the curvature concavity or convexity whilst c_i drives the initial attenuation value. Figure 5 shows different curvatures depending on the values a_i and c_i for T=500 and p_o^i = 0.75. In order to optimize the probabilities of the GA, as well as the parameters a_i and c_i of each function $p_i(t)$, we apply a meta-GA, called Additional Genetic System (AGS) to the GA, as shown in Figure 7. In the population of the AGS a candidate solution is PS_n, n=1,…,20. Each one represents the probabilities set applied to the genetic operators which are used by the GA along with the parameters a_i and c_i. Therefore each PS_n codes a vector of real values in the following way:

$$PS_n = \{\ Ps, Pc, Pm, a1, c1, a2, c2, a3, c3\}$$

Thus, we represent a population of 20 individuals by PS and it is set up as follows: PS = (PS_1,….,PS_{20}). We consider a Steady-State real-coded GA model which applies a crossover operator based on the use of fuzzy connectives [23] and a mutation random operator. The selection operator selects the best individuals (PSn) from the population in order to use them as parents for the new offspring. We use the following parameters: Pc=1.0‹ Pm=0.05 and the percentage of the population to be replaced during each generation is 30%.

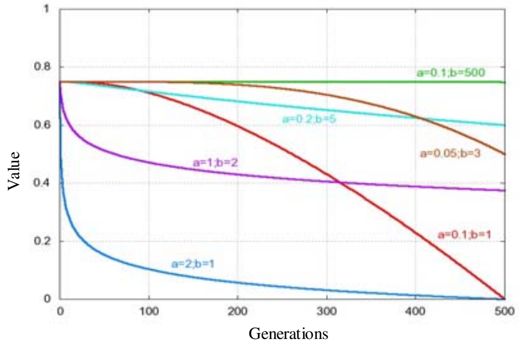


Fig. 5. Effect of the parameters a_i and c_i

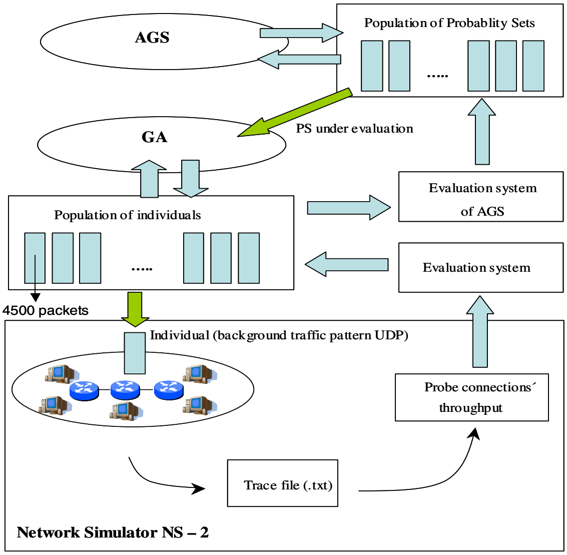


Fig. 6. Evolutionary learning of the PS of a GA

5 Results

The performance of the GA will be reviewed to drive the generation of a background traffic minimizing (critical background traffic) throughput in the computer network.

Standard statistical approach. For the standard statistical approach, where the background traffic is randomly generated according an equivalent Poisson process, we report the throughput obtained after simulating 30 times random patterns. As can see in Figure 7, the value does not change significantly, ≈ 1,5E+06 bits/sec, as new traffic patterns are randomly generated.

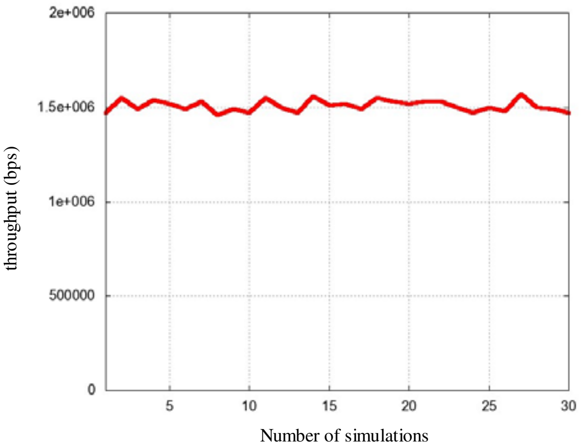


Fig. 7. Throughput of probe connections using Poisson's statistical processes

Using the static probabilities recommended. Table 3 show the results obtained when the GA uses the static probabilities recommend in [18] [19]: we have called GA-STATIC1 and GA_STATIC2 respectively. We run the GAs 30 times, each one with a maximum of 500 generations, in order to do later an experimental statistical analysis. The performance measures used are the following:

- **Average** performance: average of the lowest throughput obtained at the end of each run.
- **Generation** performance: number of generations after which improvements in solution quality were no longer obtained.

Table 3. Results obtained using the static probabilities recommended

Algorithm	Average (bps)	Generations
GA-STATIC1	655928	270
GA-STATIC2	674382	248

The lowest throughput obtained using GA-STATIC1 was 429382 bps and using GA-STATIC2 it was 502207 bps. In [18], the authors show a unique experiment and its result. The GA managed to degrade the probe connections´ throughput to 480000 bps.

Using an Adaptive Genetic Algorithm. An adaptive method presented in the literature [3] has been used, called GA-SELF (Self-adaptive control), which adapts the mutation probability during the run of the GA. We have considered the adaptation of this parameter since it can determine directly the degree of population diversity, which is the main factor to avoid the premature convergence problem [3]. The rest of the parameter values are the recommended in [4][19]. In the Self-adaptive control of Pm, an extra gen, *Pmi*, is added to the front of each individual and represents the mutation probability for all genes in the string. This gene evolves with the solution.

The values of *Pmi* are allowed to vary in the interval [0.001, 0.01] which has been chosen since it contains a wide spectrum of Pm values that were considered frequently in the literature. In this case, the average of the lowest throughput obtained at the end of each run has been 640813 bps, and the number of generations after which improvements in solution quality were no longer obtained was of 291. The lowest throughput obtained was 429382 bps 536255 bps.

Using the probabilities obtained from the AGS. When the AGS was introduced to the GA, the PS_n which obtained the highest mark was:

$$PS_{best} = \{0.7, 0.53, 0.0004, 0.38, 38.41, 0.75, 35.6, 0.57, 76.8\}$$

Later, the GA used these probabilities (in this case AGA) for each experiment. Again, we run the AGA 30 times each one with a maximum of 500 generations. The average of the lowest throughput obtained has been 438020 bps and the number of generations after which improvements were no longer obtained was of 347. The lowest throughput obtained was 304540 bps, as we can see in Figure 8.

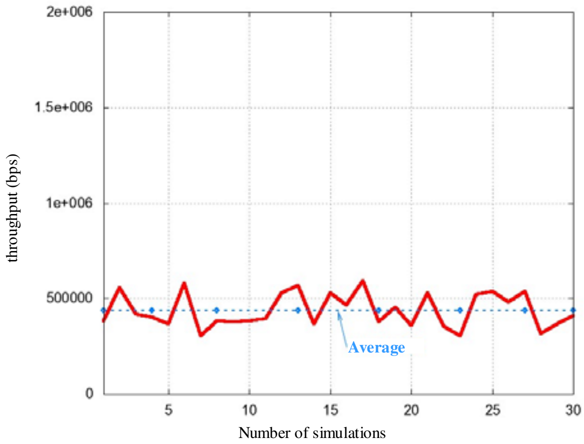


Fig. 8. Throughput using the probabilities obtained from the AGS

Statistical study. A t-student test was made in order to check if differences in the *Average* and *Generations* performance measures for AGS are significant when compared with the ones for the other algorithms. A significance level α = 0,05 was applied for the test in question. Table 4 shows the results, where we can notice significant improvements in the average throughput using AGS. A plus sign (+) denotes an improvement in the performance, a minus sign (-) a reduction, and equal sign (=) non significant differences. As can be observed, the AGS has generated a background traffic pattern which significantly degrades the computer network performance.

Table 4. t-student test results

Algorithm	Average (bps)	Generations
GA-STATIC1	655928 +	270 -
GA-STATIC2	674382 +	248 -
GA-SELF	640813 +	291 =
AGS	438020	347

6 Conclusions

The paper presents an effective approach for control parameters optimization of a Genetic Algorithm, which has been applied to a real problem.□The proposed system uses a meta-GA combined with an adaptation strategy of the GA control parameter. The results proved that, when the background traffic is driven by a GA which uses the probabilities obtained from the AGS, the computer network performance is much lower than when the traffic is generated by Poisson's statistical processes and by other algorithms. The AGS has identified the worst traffic pattern to the protocol. Using Poisson's statistical processes as models of background traffic is not possible to analyze the worst situation in a computer network. Poisson's statistical models are optimistic models to verify the computer network performance. The AGS is able to find realistic traffic loads to test the computer network. Finally, a two-sided t-test at 0,05 level of significance has been applied in order to ascertain the significant differences.

References

1. Goldberg, D.E.: Genetic Algorithms in search, optimization and Machine Learning. Addison-Wesley, New York (1989)
2. Cordón, O., Herrera, F., Hoffmann, F., Magdalena, L.: Genetic Fuzzy Systems: Evolutionary tuning and learning of fuzzy knowledge bases. Advances in fuzzy systems – Applications and theory, vol. 19. World Scientific Publishing, Singapore (2001)
3. Herrera, F., Lozano, M.: Fuzzy adaptive genetic algorithms: design, taxonomy, and future directions. Soft Computing 7, 545–562 (2003)
4. Grefenstette, J.J.: Optimization of control parameters for genetic algorithms. IEEE Transactions on Systems, Man and Cybernetics 16(1), 122–128 (1986)
5. Eiben, A.E., Michalewicz, Z., Schoenauer, M., Smith, J.E.: Parameter Control in Evolutionary Algorithms. In: Parameter Setting in Evolutionary Algorithms. Springer, Heidelberg (2007)
6. De Jong, K.: An analysis of the behaviour of a class of genetic adaptive systems. PhD thesis, University of Michigan (1975)
7. Grefenstette, J.J.: Optimization of control parameters for genetic algorithms. IEEE Transactions on Systems, Man and Cybernetics 16(1), 122–128 (1986)
8. Bramlette, M.F.: Initialization, mutation and selection methods in genetic algorithms for function optimization. In: Proceedings of the Fourth International Conference on Genetic Algorithms, pp. 100–107. Morgan Kaufmann, San Mateo (1991)
9. Eiben, A.E., Hinterding, R., Michalewicz, Z.: Parameter control in evolutionary algorithms. IEEE Transactions on Evolutionary Computation 3, 124–141 (1999)

10. Cicirello, V.A., Smith, S.F.: Modeling GA performance for control parameter optimization. In: Proceedings of the Genetic and Evolutionary Computation Conference, pp. 235–242. Morgan Kaufmann Publishers, Las Vegas (2000)
11. Michalewicz, Z., Schmidt, M.: Parameter Control in Practice. In: Parameter Setting in Evolutionary Algorithms. Springer, Heidelberg (2007)
12. Wolpert, D.H., MacReady, W.G.: No free lunch theorems for optimization. IEEE Transactions on Evolutionary Computation 1(1), 67–82 (1997)
13. Hinterding, R., Michalewicz, Z., Eiben, G.: Adaptation in Evolutionary Computation: A Survey. In: Proc. of the IEEE Conference on Evolutionary Computation, pp. 65–69 (1997)
14. De Jong, K.: Parameter Setting in EAs: a 30 year Perspective. Parameter Setting in Evolutionary Algorithms. Springer, Heidelberg (2007)
15. Hui, J.: Switching and Traffic Theory for Integrated Broad Band Networks. Kluwer Academic Publisher, Dordrecht (1990)
16. Karagiannis, T., Molle, M., Faloutsos, Broido, A.: A nonstationary poisson view of internet traffic. Proc. of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), Hong Kong, vol. 3, pp. 1558–1569 (2004)
17. Cao, J., Cleveland, W., Lin, D., Sun, D.: Internet traffic Tends Toward Poisson and Independent as the Load Increases. In: Holmes, C., Dennison, D., Hansen, M., Yu, B., Mallick, B. (eds.) Nonlinear Estimation and Classification 2002. LNS, pp. 83–109. Springer, Heidelberg (2003)
18. Corne, D.W., Oates, M.J., Smith, G.D.: Telecommunications Optimization: Heuristic and Adaptive Techniques. John Wiley and Sons Ltd., Chichester (2000)
19. Karthik, S., Jawajar, V., Chidambararajan, B., Srivatsa, S.K.: Performance of TCP over satellite networks under severe cross-traffic using GA. International Journal Mobile Communications 2(4), 382–394 (2004)
20. The Network Simulator -ns-2, `http://www.isi.edu/nsnam/ns`
21. Fernández-Prieto, J.A., Velasco, J.R.: Application of Genetic Algorithms in the research of the optimum probabilities of the genetic operators. In: 8th International Conference on Information Processing and Management of Uncertainty in Knowledge Based Systems (IPMU), pp. 291–297 (2000)
22. GAlib, `http://lancet.mit.edu/ga`
23. Herrera, F., Lozano, M., Verdegay, J.L.: The Use of Fuzzy Connectives to Design Real-Coded Genetic Algorithms. Mathware and Soft Computing 1(3), 239–251 (1995)

On the Application of a Novel Grouping Harmony Search Algorithm to the Switch Location Problem

Sergio Gil-Lopez[1], Javier Del Ser[1], Itziar Landa[1], Laura Garcia-Padrones[1],
Sancho Salcedo-Sanz[2], and Jose A. Portilla-Figueras[2]

[1] TECNALIA-TELECOM
48170 Zamudio (Bizkaia, Spain)
{sgil,jdelser,ilanda}@robotiker.es,
[2] Department of Signal Theory and Communications, Universidad de Alcala
28871 Alcala de Henares (Madrid, Spain)
{sancho.salcedo,antonio.portilla}@uah.es

Abstract. This paper presents the adaptation of a novel heuristic algorithm to the Switch Location Problem (SLP), a NP-hard problem where a set of distributed terminals, with distinct rate demands, is to be assigned to a fixed number of concentrators subject to capacity constraints. Each terminal must be assigned to one and only one concentrator while keeping the overall rate demanded from such concentrator below its maximum capacity. Related literature demonstrates that the inclusion of the so-called *grouping* concept into the allocation algorithm is essential when dealing with this specific kind of optimization scenarios. As such, previous studies introducing Grouped Genetic Algorithms (GGA) combined with local search and/or repair methods show that their proposed allocation procedure alleviates significantly the computational complexity required by an exhaustive search strategy for the SLP problem, while outperforming other hybrid heuristic algorithms. In this manuscript, a novel Grouped Harmony Search (GHS) algorithm designed for the SLP paradigm is hybridized with both a local search method and a technique aimed at repairing the solutions iteratively supplied by the heuristic process. Extensive Monte Carlo simulations assess that our proposal provides faster convergence rate and better statistical performance than the previously proposed GGA, specially when the size of the SLP scenario increases.

Keywords: ANLP/SLP, Heuristic Algorithm, Genetic Algorithm, Harmony Search.

1 Introduction

The last decade has witnessed an abrupt increase of the number of users simultaneously accessing and exploiting communication resources, which has risen the importance of efficiently designing networks' infrastructures and topologies

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 662–672, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

to its maximum. This assertion is buttressed by the flurry of densely-deployed communication technologies such as the ever-trendy Wireless Sensor Networks (WSN) or the mobile telecommunication networks.

In this context, among the plethora of problems related to network planning it is worth mentioning the design of fixed network topology [1], optimum base station location [2], Access Node Location Problem (ANLP) [3] and the Terminal Assignment (TA) problem [4], all of which constitute by themselves NP-hard problems. NP-hardness implies that the search for an analytical optimum solution cannot be guaranteed to be found in a polynomial time, the reason being that the solution space increases exponentially with the number of inputs. It was not until the mid 80's when the application of heuristic and/or evolutionary methods were extensively applied to NP-hard problems, mainly due to their near-optimum performance and easy implementation and adaptation to different scenarios (e.g. Tabu Search [5], [6], Simulated Annealing [7] or Genetic Algorithm [8]).

Let us concentrate on the so-called *Switch Location Problem* (SLP), which gravitates on assigning a given set of terminal to a given set of concentrator by minimizing the total average distance (and hence the cost) between terminals and concentrators. Furthermore, only one concentrator can be assigned to one terminal and the capacity of each concentrator must satisfy the overall rate requirements demanded by its assigned terminals. These additionally imposed constraints implies that a global search strategy must be replaced by a restricted search procedure, capable of minimizing the average distance while accounting for the capacity requirements of the scenario at hand. Notice that in the related literature both SLP and ANLP are distinct albeit related version of the Terminal Assignment problem, where a set of M concentrators is drawn from $N > M$ terminals, and the $N-M$ remaining terminals are linked to the M concentrators under a capacity constraint. SLP stands for the case when the value of M is fixed and known beforehand, whereas ANLP generalizes the optimization problem by considering a variable M. As a means to efficiently solve the aforementioned SLP paradigm, hybrid algorithms mixing global search techniques with local techniques were proposed in [4,9]. Within this line of research, the concept of Grouping Genetic Algorithms (GGA) was first introduced by [10,11] and recently applied to the ANLP problem in [3].

This paper advances over the state of the art by proposing the adaptation of the recent Harmony Search (HS) heuristic algorithm to the SLP paradigm. First coined by Zong *et al.* in [12], the HS algorithm mimics the behavior of a music orchestra in the process of music composition. Several optimization problems have benefited from the excellent performance of HS for scenarios of specially high complexity, e.g. water network design [13], multicast routing [14] or multiuser detection [15,16]. To adapt the global search characteristic featured by the HS algorithm to the restricted solution space of the SLP problem tackled herein, it is necessary to include two additional concepts in the nominal HS procedure: 1) a local search method, and 2) a repair criterion of proposed solutions not fulfilling the imposed capacity constraints. In addition, the grouping concept is utilized to encode the iteratively obtained solutions, which gives birth to the Grouping Harmony Search (GHS) allocation strategy here proposed. Monte Carlo simulation results show that the performance of GGA reported in [17] is beaten by that of GHS for a broad range of SLP scenarios, in terms not only of the optimality of the provided solution but also of its computational complexity.

The rest of the manuscript is structured as follows: the problem formulation of the SLP problem is presented in Section 2, whereas Section 3 details the main characteristics of the proposed Grouping Harmony Search (GHS) algorithm. Next, Section 4 discusses a comparison study between the proposed algorithm and the Grouping Genetic procedure for different network configurations. Finally, concluding remarks are drawn in Section 5.

2 Problem Formulation

Let us mathematically define the SLP problem by assuming a set of N terminals $\{l_1, l_2, \ldots, l_N\}$ with associated rate requirements or *weights* $\{w_1, w_2, \ldots, w_N\}$. Each such terminals should be assigned to any of $M \leq N$ concentrators $\{r_1, r_2, \ldots, r_M\}$ drawn out from the N terminals. We assume that such concentrators have maximum capacities $\{p_1, p_2, \ldots, p_M\}$, that $w_i < \min(p_1, p_2, \ldots, p_M)$ $\forall i \in \{1, \ldots, N\}$, and that concentrator nodes should be chosen from the complete set of N nodes because terminal and concentrator share the same network infrastructure. If we further consider that only one concentrator can be assigned to a given terminal, the terminal-concentrator assignment policy should be done by minimizing the total sum of distances between each terminal and its selected concentrator while satisfying, at the same time, the capacity constraint. This optimization problem can be split in 1) connecting the set of terminals to a given set of concentrators, and 2) selecting the nodes which act as concentrators.

All nodes are randomly spread over a $K \times K$ grid. We can then define a $N \times N$ symmetric matrix $\mathbf{D}$ such that each entry $d_{i,j}$ represents the euclidean distance from node i to node j. Let us define matrix $\mathbf{X}$ with binary entries $x_{i,j}$ such that $x_{i,j} = 1$ if terminal i is assigned to concentrator j and $x_{ij} = 0$ otherwise. By using this notation the SLP problem reduces to finding the matrix $\mathbf{X}$ which satisfies, for a given N and M,

$$\min\left(\sum_{j=1}^{M}\sum_{i=1}^{N} d_{ij} \cdot x_{ij}\right), \tag{1}$$

subject to

$$\sum_{i=1}^{N} w_{ij} \cdot x_{ij} \leq p_j \qquad j = 1, \ldots, M, \tag{2}$$

$$\sum_{j=1}^{M} x_{ij} = 1 \qquad i = 1, \ldots, N \tag{3}$$

Observe that expression (1) establishes the metric or fitness function that allows quantifying the cost of each network configuration, while equations (2) and

(3) represent the constraints imposed in the SLP scenario. The first expression ensures that the requirements of the terminals associated to a certain concentrator cannot exceed its maximum capacity, whereas the second constraint accounts for the fact that each terminal can be connected only to one concentrator. Also notice that for this constrained optimization problem a global search technique to optimize the search over the $\binom{M}{N}$ possible solutions is not as adequate as an optimized restricted technique well-suited to meeting the constraints of expressions (2) and (3). The next section details the adaptation of the novel heuristic Harmony Search algorithm towards efficiently solving this optimization problem, which requires a specific encoding of the possible solutions and the inclusion of a local search and repair methods.

3 Grouping Harmony Search for the SLP Problem

The *grouping* encoding strategy finds its roots on partitioning a set of items into several disjoint subsets or, equivalently, on grouping the members of a set into several subsets by following certain criteria (possibly) based on constraints. The first proposed Grouping Genetic Algorithm (GGA) was published by Falkenaurer in [10,11], where it was applied to solve the “Bin Packing and Line Balancing” NP-problem. More than 15 years later, the concept of Grouping has been proven to be essential in the resolution of SLP and/or ANLP problems by Alonso-Garrido *et al.* in [3]. Following the notation and structure proposed therein, in this contribution we transform the Harmony Search heuristic algorithm into a Grouping Harmony Search (GHS) procedure. Each proposed solution vector $\mathbf{s} = (\mathbf{s}_x \mid \mathbf{s}_y)$ will be divided into the assignment part ($\mathbf{s}_x$) and the grouping part ($\mathbf{s}_y$). The assignment part consists of N integer indices from the set $\{1, \ldots, M\}$, which denote to which concentrator (from the $\mathbf{s}_y$ set) is assigned each of the N terminals. On the other hand, the $\mathbf{s}_y$ grouping part is built by concatenating M integer indices from the set $\{1, \ldots, N\}$, denoting which nodes act as concentrators.

As introduced in Section 1, the Harmony Search (HS) algorithm is based on mimicking the behavior of a music orchestra in their attempt to achieve the best harmony. In this seeking process, Harmony Search works with a set of φ possible solutions or harmonies commonly denoted as Harmony Memory (HM), which are evaluated at each iteration under an aesthetic point of view. The Harmony Memory is updated whenever any of the φ improvised harmonies at a given iteration sounds *better* (under a certain fitness criterion) than any of the φ harmonies kept from the previous iteration. This procedure is iteratively repeated until the best harmony is reached or alternatively, until a fixed number of attempts or iterations are completed. For the sake of conformity with the notation in [12], we will hereafter refer to a possible candidate vector (i. e. s_x) as *harmony*, and *note* will stand for any of its compounding entries.

The harmony improvisation process of the seminal HS algorithm is controlled by just two parameters: 1) *Harmony Memory Considering Rate*, HMCR; and 2) *Pitch Adjusting Rate*, PAR. Similar to [16], in this contribution the proposed improvisation procedure differs from the original HS implementation by introducing a third parameter (Random Selection Rate, RSR), which allows for an improved control of the tradeoff between the explorative and the exploitative behavior of the algorithm.

The flow diagram of the algorithm here proposed is schematically shown in Figure 1, and consists of four steps:

A. The **Initialization** process is only executed at the first iteration. At this point, since no a priori knowledge of the solution is assumed the harmony notes (i.e. the entries of $\mathbf{s}_x$) are filled with values picked randomly from the corresponding alphabet $\{1, \ldots, M\}$.

B. The **Improvisation** process is sequentially applied to each note of the complete set of harmonies. As opposed to the nominal HS scheme three arbitrary parameters are used to control the proposed method:
   - The Harmony Memory Considering Rate, HMCR $\in [0, 1]$, which establishes the probability that the new value for a note is drawn from the values of the same note taken in all the other $\varphi - 1$ harmonies included in the Harmony Memory.
   - The Random Selection Rate, RSR $\in [0, 1]$, which stands for the probability that the proposed new value for a note is selected randomly from the corresponding alphabet (in general it will be set different from the complementary probability 1-HMCR used by the nominal HS algorithm).
   - The Pitch Adjusting Rate, PAR $\in [0, 1]$, which sets the probability that the new note value is picked from its neighbor value in the alphabet.

C. The existence of capacity limits at the concentrators requires the transformation of the global search behavior of the algorithm into a constrained search process. Heretofore the search is not limited to a certain set of valid candidates; in other words, the procedure does not consider any of the conditions imposed by expressions (2) and (3). Therefore, the iterative global search process is not as efficient as an hybridized approach. To overcome this issue, it is necessary to include two additional processes:
   - The so-called *GreedyExp* algorithm is the **local search method** adopted in this work, which was first proposed by Salcedo-Sanz *et al.* in [18,3] as an optimized version of the original *Greedy* algorithm [19].
   - The **repair criterion** in [18,3] is applied to the harmonies when capacity constraints are not satisfied.

D. At each iteration the quality **evaluation** of the improvised harmony memory is made based on the fitness function in expression (1). Once the local search and repair criteria are applied, if any of the proposed melodies does not satisfy the capacity constraints its metric are penalized to avoid its future inclusion in the Harmony Memory. Then, based on these metric evaluations and their comparison with the fitness of harmonies from previous iterations, the φ best harmonies are kept and the Harmony Memory is hence **updated**.

D. A simple **stop criterion** is selected for the scenario at hand: the algorithm finishes when a fixed number of iterations $\mathcal{I}$ is reached.

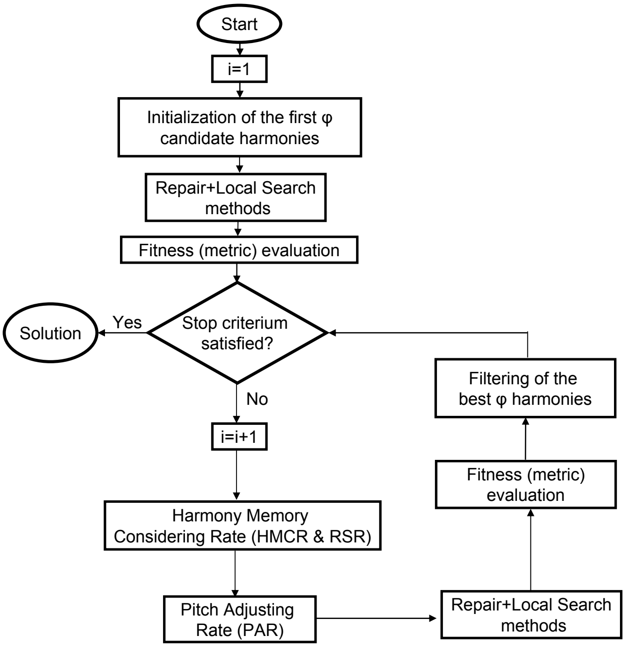

Start
i=1
Initialization of the first φ candidate harmonies
Repair+Local Search methods
Fitness (metric) evaluation
Stop criterium satisfied?
Yes
Solution
No
i=i+1
Harmony Memory Considering Rate (HMCR & RSR)
Pitch Adjusting Rate (PAR)
Repair+Local Search methods
Fitness (metric) evaluation
Filtering of the best φ harmonies

Fig. 1. Flow diagram of the proposed GHS algorithm (i denotes iteration)

Before proceeding to the simulation results, it should be emphasized that the proposed method not only adapts the Harmony Search algorithm from [12] to the SLP problem, but works rather differently than other previous GGA-related works (e.g. [3]) where the selection, crossover and mutation processes are jointly applied to the $\mathbf{s}_x$ and $\mathbf{s}_y$ vectors. In the present scheme, the algorithm improvises the melodies included in the Harmony Memory by applying the improvisation process only to the $\mathbf{s}_x$ part of the solution (i.e. without considering the $\mathbf{s}_y$ vector). After the $\mathbf{s}_x$ vector is modified, $\mathbf{s}_y$ is built by selecting as concentrator such node that minimizes the sum of distances from itself to all terminals grouped in the corresponding $\mathbf{s}_x$ assignment part.

4 Simulation Results

In order to assess the performance of the proposed hybrid GHS scheme when applied to the SLP problem, a comparison study between GHS and GGA has been done based on extensive Monte Carlo simulations. In [18,17] it is shown that the performance rendered by the application of GGA to the SLP paradigm considered herein is significantly better than that of previous related works where alternate evolutionary algorithms are considered. Therefore, the present comparison study is based on the results and scenarios published in [17].

Fairness in this study is ensured by utilizing the same physical locations (x- and y coordinates), rate demands and maximum capacities of the nodes for both

Table 1. Parameters of the simulated scenarios

Instance	N	M	Grid
1	20	3	500 × 500
2	40	4	500 × 500
3	50	4	500 × 500
4	60	5	500 × 500
5	80	8	500 × 500
6	90	9	500 × 500
7	100	10	500 × 500
8	110	10	500 × 500
9	150	15	500 × 500

GGA and GHS algorithms. Furthermore, the scalability of the proposed heuristic allocation procedure is verified by considering 9 different network instances: from the simplest $N = 20$ and $M = 3$ to the most complex $N = 150$ and $M = 15$. Table 1 details the parameters for all problem dimensions handled in this paper. In all these scenarios the nodes coordinates are randomly generated in a 500×500 grid, whereas terminal rate requirements are drawn from a normal distribution with mean 10 and standard deviation 5. Besides, as a means to guarantee the existence of a solution in the setup, i.e.

$$\sum_{i=1}^{N} w_i < \sum_{j=1}^{M} p_j, \tag{4}$$

the capacities of the concentrators $\{p_j\}_{j=1}^{M}$ are generated as a function of terminal requirements by setting

$$p_j = \frac{1,1 \cdot \left(\sum\limits_{i=1}^{N} w_i \right)}{M} \tag{5}$$

where w_i is the rate requirement of the i-th terminal, and N and M are the overall number of terminals and concentrators, respectively. On the other hand, the selection of the parameters (HMCR, RSR, PAR) and the maximum number of iterations $\mathcal{I}$ for the simulated GHS approach are based on a previous optimization study made for the most complex scenario ($N = 150$, $M = 15$). A range from 0.01 to 0.99 for the three aforementioned parameters was simulated in more than 40 different sets of network realizations. The best performance was obtained for (HMCR, RSR, PAR)=(0.1, 0.07, 0.03), values that will be hereafter utilized for the comparison study.

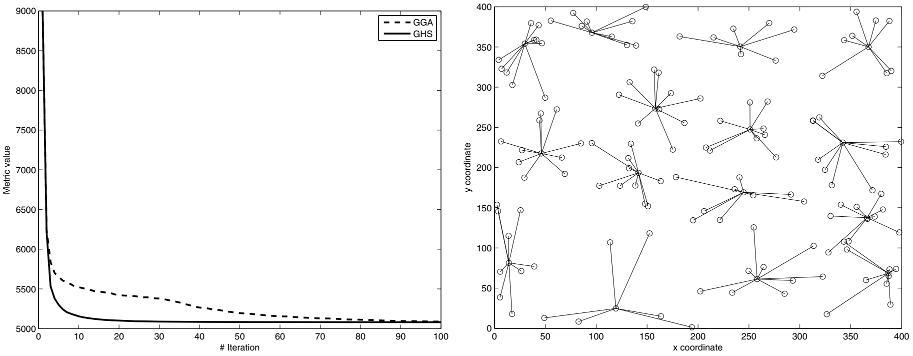
Furthermore, the computational cost is set the same for the GGA and GHS allocation techniques. In this study, both algorithms work without any previous knowledge about the scenario and with the same memory size (i.e. the population size of the GGA – 50 chromosomes – equals that of the Harmony Memory in the GHS technique). However, the maximum number of iterations for GHS is

Table 2. Statistical metric results (best/average/standard deviation) for GGA and GHS in the different SLP instances detailed in Table 1

SLP instance	GGA	GHS	Theoretical lower bound
1	1419/1419/0	1419/1419/0	1395
2	2455/2455/0	2455/2455/0	2403
3	3712/3712/0	3712/3712/0	3684
4	3800/3813/17	3800/3800/0	3706
5	3806/3819/18	3806/3807/1	3713
6	3792/3807/16	3792/3795/10	3684
7	4455/4498/26	4455/4464/13	4359
8	4724/4745/28	4724/4728/4	4563
9	5059/5127/47	5059/5080/19	4823

set to $\mathcal{I} = 100$, as opposed to the GGA proposed in [3] which iterates until a maximum number of 200 generations is reached. Consequently, the GHS results later detailed are obtained with half the computational complexity of the GGA approach for the same SLP scenario.

Table 2 summarizes the metric results obtained by both algorithms for the SLP instances detailed in Table 1. Notice that the last column indicates the theoretical lower bound when no capacity limits are assumed for the concentrator nodes. Note that in most cases this theoretical lower bound is unattainable if capacity requirements are imposed. For each case, the results are obtained by averaging the metric – as defined in expression (1) – over 20 and 50 different realizations of the network. Observe that the three simplest scenarios (1 to 3) render the same statistical results for GGA and GHS. However, notice that at



(a) (b)

Fig. 2. (a) GGA and GHS average metric (over 50 network realizations) versus iteration index for the most complex scenario (N, M)=(150, 15); (b) Example of obtained optimum distribution for the same SLP scenario instance 4, the standard deviation of the GHS approach is still equal to zero (i.e. the algorithm provides the same minimum metric for all all Monte Carlo simulated network realizations), whereas that of the GGA technique is bounded away from 0. As for instances 5 to 7, the same minimum metric is reached, but GHS provides better average results and a lower standard deviation, difference that gets even higher for the last two network instances. These results for GHS are obtained at half the computational complexity of GGA, which enlightens the benefits entailed by our proposal.

Let us elaborate further on the convergence behavior of GGA and GHS by considering Figure 2, where the average metric of both algorithms is plotted versus the iteration index for the most complex scenario ($N = 150$, $M = 15$). Observe that GHS has a faster convergence rate than GGA, which motivates reducing the maximum number of iterations $\mathcal{I}$ for GHS (in fact, in light of these simulation results one could further decrease $\mathcal{I}$ below the selected value of 100, since the average metric is kept constant beyond 50 iterations of the GHS algorithm). Finally, Figure 2.b depicts an example of the optimum network configuration (N, M)=(150, 15).

5 Conclusions

In this paper we have proposed a novel hybrid grouping heuristic algorithm for solving the so-called Switch Location Problem. Our approach is based on the Harmony Search global search algorithm in conjunction with a *GreedyExp* Local Search criterion and a repair solution method. Based on the parameters governing the behavior of the algorithm (selected as a result of an intensive optimization study), simulation results show that GHS outperforms previous GGA approaches in terms of convergence rate, computational complexity and distance to the theoretical metric lower bound assuming no capacity constraints. Consequently, the overall cost of the network design is reduced with respect to other avantgarde techniques.

Further work on this topic will focus on extending the applicability of GHS to the more general Access Node Location Problem (ANLP), where the number of concentrators is not fixed. Research effort will also be conducted towards the inclusion of perturbing criteria or the dynamic adjustment of the GHS parameters during the iterative process, as means to narrow the gap between the obtained average metric results and the capacity-unconstrained theoretical lower bound.

Acknowledgments

This work was supported in part by the Spanish Ministry of Science and Innovation through the CONSOLIDER-INGENIO 2010 (CSD200800010), the Torres-Quevedo (PTQ-09-01-00740, PTQ-06-01-0159) funding programs, as well as by the Basque Government through the ETORTEK Programme (*Future Internet* EI08-227 project).

References

1. Pierre, S., Elgibaoui, A.: Improving Communications Networks' Topologies using Tabu Search. In: 22nd Annual Conference on Local Computer Networks (LCN 1997), pp. 44–53 (1997)
2. Calegari, P., Guidec, F., Kuonen, P., Wagner, D.: Genetic Approach to Radio Network Optimization for Mobile Systems. In: IEEE Vehicular Technology Conference, vol. 2, pp. 755–759 (1997)
3. Alonso-Garrido, O., Salcedo-Sanz, S., Agustin-Blas, L.E., Ortiz-Garcia, E.G., Perez-Bellido, A.M., Portilla-Figueras, J.A.: A Hybrid Grouping Genetic Algorithm for the Multiple-ype Access Node Location Problem. In: Corchado, E., Yin, H. (eds.) IDEAL 2009. LNCS, vol. 5788, pp. 376–383. Springer, Heidelberg (2009)
4. Salcedo-Sanz, S., Yao, X.: A Hybrid Hopfield Network-Genetic Algorithm Approach for the Terminal Assignment Problem. IEEE Transactions on Systems, Man, and Cybernetics, PartB: Cybernetics 34(6), 2343–2353 (2004)
5. Glober, F.: Tabu Search–Part I. ORSA Journal on Computing 1(3), 190–206 (1989)
6. Glober, F.: Tabu Search–Part II. ORSA Journal on Computing, 2(1), 4–32 (1989)
7. Kirkpatrick, S., Gelatt, C.D., Vecchi, M.P.: Optimization by Simulated Annealing. Science, New Series 220(4598), 671–680 (1983)
8. Holland, J.H.: Adaptation in Natural and Artificial Systems. University of Michigan Press (1975)
9. Khuri, S., Chiu, T.: Heuristic Algorithms for the Terminal Assignment Problem. In: Computer and Operations Research, pp. 17–23 (1997)
10. Falkernauer, E.: The Grouping Genetic Algorithms-Widening the Scope of the GAs. Belgian Journal of Operations Research, Statistics and Computer Science 33, 79–102 (1993)
11. Falkenauer, E.: A New Representation and Operators for Genetic Algorithms Applied to Grouping Problems. In: Evolutionary Computation, pp. 123–144. MIT Press, Massachusetts (1994)
12. Geem, Z.W., Hoon Kim, J., Loganathan, G.V.: A New Heuristic Optimization Algorithm: Harmony Search. Simulation 76(2), 60–68 (2001)
13. Geem, Z.W.: Optimal Cost Design of Water Distribution Networks using Harmony Search. Engineering Optimization 38(3), 259–277 (2006)
14. Forsati, R., Haghighat, A.T., Mahdavi, M.: Harmony Search Based Algorithms for Bandwidth-Delay-Constrained Least-Cost Multicast Routing. Computer Communications 31(10), 2505–2519 (2008)
15. Gil-Lopez, S., Del Ser, J., Olabarrieta, I.: A Novel Heuristic Algorithm for Multiuser Detection in Synchronous CDMA Wireless Sensor Networks. In: IEEE International Conference on Ultra Modern Communications, pp. 1–6 (2009)
16. Gil-Lopez, S., Del Ser, J., Garcia-Padrones, L.: Harmony Search Heuristics for Quasi-Asynchronous CDMA Detection with M-PAM Signalling. Submitted to 2nd International Conference on Mobile Lightweight Systems (MOBILIGHT), Barcelona, Spain (2009)
17. Alonso-Garrido, O., Portilla-Figueras, J.A., Agustin-Blas, L.E., Salcedo-Sanz, S.: Localizacion Optima de Nodos de Acceso en el Despliegue de Redes de Comunicacion: Aplicacion de un Algoritmo Evolutivo de Agrupaciones. In: XXIV National Assembly of the International Union of Radio Science, URSI (2009)

18. Salcedo-Sanz, S., Portilla-Figueras, J., Ortiz-Garcia, E.G., Perez-Bellido, A.M., Thraves, C., Fernandez-Anta, A., Yao, X.: Optimal Switch Location in Mobile Communication Networks using Hybrid Genetic Algorithms. Applied Soft Computing 8, 1486–1497 (2008)
19. Abuali, F.N., Schoenefeld, D.A., Wainwrigght, R.L.: Terminal Assignment in a Communications Network using Genetic Algorithm. In: 22nd Annual ACM Computer Science Conference, pp. 74–81 (1994)

Adaptive Weighted Round Robin (AWRR) Scheduling for Optimization of the Wireless Medium Virtualisation

Gorka Hernando, Susana Pérez, and José María Cabero

TECNALIA-Telecom, Technology Center, Zamudio, 48170, Spain
Tel.: +34 94 6002266, Fax: +34 94 6002299
`{ghernando,sperez,jmcabero}@robotiker.es`
`http://www.robotiker.es/`

Abstract. Network virtualisation has been recently presented as a mean to overcome the saturation of the current Internet by sharing the same infrastructure by different network operators. This work considers virtualisation of the wireless medium, a way to share common network physical resources by different Virtual Operators based on a Time Division Multiple Access technique. We propose an Adaptive Weighted Round Robin scheduler as a means to optimize the assignment of time slots to each virtual operator and improve the performance of the system. End-to-end delay and packet loss are the metrics used in this paper to show the potential and limitations of wireless virtualisation as a way to increase the network usage. This research is presented as a simulation-based study developed over the widely used NS2 network simulator. Different scenarios and network topologies are considered in order to assess the benefits of using the proposed scheduler.

Keywords: Virtualisation, Adaptive TDMA Scheduler, Optimization, Weighted Round Robin.

1 Introduction

Many new necessities and requirements have been requested by the final users during the last years, some of them with conflicting goals and policies, making the current Internet network paradigm almost impossible to achieve. Therefore, network virtualisation has been recently presented as a key concept for the construction of the Future Internet because of its potential to allow multiple network architectures coexist [1][2]. Virtualisation is based on sharing a common physical substrate by several providers running their own services in a fully isolated and protected way. Many different research lines are boosted nowadays regarding network virtualisation: innovative network architectures [3], efficient embedding algorithms for the creation of virtual networks [4][5], techniques for the virtualisation of the physical resources [6][7], among others.

The wireless medium is a common physical resource that does not purely belong to a specific node but the whole network itself. In general, virtualisation techniques for the wireless medium look for the shared use of a wireless transmission medium in a coordinated way [8], i.e. each virtual operator (VO) has at its disposal the wireless medium during specific times (Time Division Multiple Access (TDMA)), frequencies

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 673–684, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

(Frequency Division Multiple Access (FDMA)), codes (Code Division Multiple Access (CDMA)) and so on.

Our research focuses on the TDMA virtualisation of the wireless medium, based on a Round Robin (RR) scheduling algorithm [9]. In this approach, the scheduler divides the usage of the common resource into equal time slots (TS), each one assigned to a particular VO. The transmission frame is formed by all the individual pieces, and it is conformed by the repeated sequence of consecutive TSs, such that the time to finish a complete round (called 'quantum' in the following) will be the summation of the individual TSs. Weighted RR (WRR) is a special case of RR scheduling where the VOs are characterized by their weights, $W(VO_i)$. The $W(VO_i)$ value defines the percentage of quantum that VO_i will get. So the TS assigned to each VO is obtained as the product of the quantum by its $W(VO_i)$. Some particular situations could provoke undesired effects (non optimal performance) in this kind of systems. For instance, VO_A stops sending data after a long-lived transmission. Even if VO_A is not using its TS, this cannot be used by any other VO in place, although a certain VO_B could be suffering from congestion problems or so. Thereby, classical RR and WRR techniques are not covering an optimal sharing among VOs, since the duration of the TSs is somehow fixed and cannot be adapted to the network dynamics that might occur.

In this work an Adaptive WRR (AWRR) scheduler is presented. Our efforts aim at optimizing the use of the quantum time, improving the performance of the shared medium. While certain VOs are whether not transmitting or sending traffic at low speed (they do not exhaust their own TS), the AWRR algorithm readjusts the weights and tries to give some extra time (which is made free by the VO who does not consume its whole assignment) to other VOs. Thus, the objective of our work is to give some favour in terms of Quality of Service (QoS) to the VOs with higher transmission constraints (peaks of traffic, demanding applications, …), but without penalizing the others.

This paper is organized as follows: the outline of the TDMA scheduler used as basis is presented in Section 2, whereas Section 3 is focused on the analysis of the proposed adaptive WRR algorithm. Section 4 discusses the scenarios followed by the main simulation results and, finally, concluding remarks are drawn in Section 5.

2 TDMA Scheduler Description

A TDMA scheduler scheme similar to the one we propose here was previously validated and evaluated as the running process for a single wireless node in Matlab [10]. The objective of this mathematical implementation was to validate the WRR model as compared to the M/M/S/K systems. In this paper we assess the benefits of an AWRR scheduler in the interconnection of several nodes in different network topologies.

When the sharing is planned in a time slotted way, the situation that we are interested in corresponds to a generic node receiving traffic coming from different VOs. The traffic management inside each node consists in storing the arriving traffic packets in specific VO queues until the TDMA scheduler sends them to the wireless interface to be transmitted. The selection of these packets is done depending on the scheduling technique and the policies applied to the different types of traffic.

The basis of the scheduling algorithm proposed is depicted in Fig 1. From left to right, the whole system starts running when the arrival of traffic packets at the VO queues is produced. The system consists of the following main modules:

- *Traffic Generator (TG):* it creates the network traffic based on models [11][12] that generate arrival instants and duration intervals for all the packets of each type such as: VoIP, IPTV, HTTP, FTP, etc. The starting time of every traffic associated to a particular VO is random inside the quantum time.

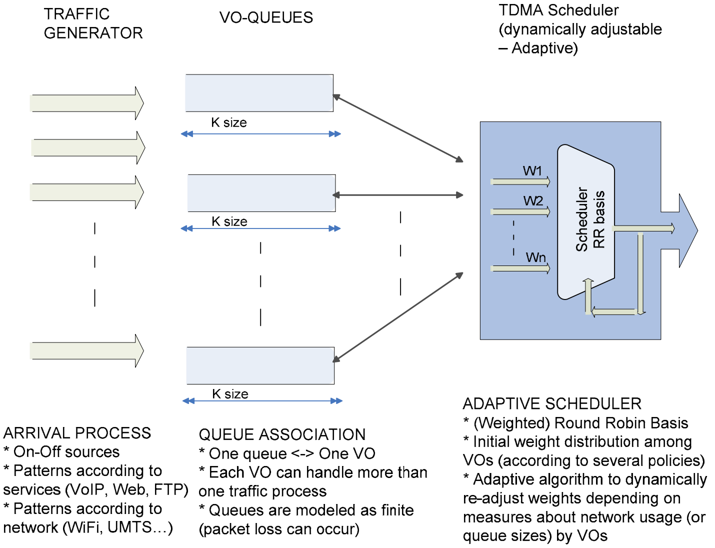

TRAFFIC GENERATOR
VO-QUEUES
TDMA Scheduler (dynamically adjustable – Adaptive)
K size
K size
K size
W1
W2
Wn
Scheduler RR basis
ARRIVAL PROCESS
* On-Off sources
* Patterns according to services (VoIP, Web, FTP)
* Patterns according to network (WiFi, UMTS...)
QUEUE ASSOCIATION
* One queue <-> One VO
* Each VO can handle more than one traffic process
* Queues are modeled as finite (packet loss can occur)
ADAPTIVE SCHEDULER
* (Weighted) Round Robin Basis
* Initial weight distribution among VOs (according to several policies)
* Adaptive algorithm to dynamically re-adjust weights depending on measures about network usage (or queue sizes) by VOs

Fig. 1. AWRR scheduler scheme

- *VO Queues*: each node consists of a number of queues equal to the number of VOs running on it and one additional queue dedicated to network management issues, i.e. ARP, Routing, etc. The key concept here is the univocal correspondence between queues and VOs. All these VO queues receive the incoming packets generated by the TG and store them until they are requested by the TDMA Scheduler. The VO queues considered are finite First Input First Output (FIFO) arrays. The limitation in the size is important because it makes packet losses possible and realistic.

  The sending of management packets is prioritized over data packets, so whenever there is a packet in this queue it will be sent as soon as possible with pre-emptive priority. Thus, the management queue does not need an own time slot and it is not considered within the AWRR algorithm.

- *TDMA Scheduler:* all the VO queues are managed by the TDMA scheduler that is in charge of allowing a specific VO queue to serve the packets to be transmitted. The TDMA Scheduler follows an AWRR discipline, i.e., it initially assigns a W(VO_i) per VO, being these values equal (RR) or different (WRR). The number of served packets depends on their size and the TS duration. In order to optimize the end-to-end delay and reduce the ratio of lost packets because of queue overflows, the scheduler readapts the weights depending on the queue occupation of each VO. Specific features of the AWRR algorithm will be explained in section 3.

3 The Adaptive Weighted Round Robin Algorithm

Trying to optimize the response of the TDMA scheduler, the proposed AWRR algorithm recalculates the weights assigned to each VO depending on the average number of packets enqueued during a certain time interval. If a certain VO stores in its queue a large number of packets during the time of analysis it will be granted with a larger $W(VO_i)$, so that the average end-to-end delay of this traffic can be reduced, improving the performance of the network. It must be noticed that this extra $W(VO_i)$ is obtained from idle intervals of other VOs, so the quantum time remains unchanged. That way, if a VO does not transmit anything for a long time, its $W(VO_i)$ would be decreased to 0 milliseconds. However, there is a restriction that the reduction of a $W(VO_i)$ can only be performed if this new value is greater than (at least equal to) the minimum weight, $MW(VO_i)$, arranged by contract. This policy tries to reflect that a certain VO may have a certain minimum QoS pre-arranged (minimum guaranteed TS) in the contract specification for its operation of the virtualised resource.

The adaption process can be triggered periodically every time-window interval, i.e. every 5 completed quantum times, or due to a certain amount of packets served, i.e. every 250 packets transmitted. The implications of choosing one method or the other will be assessed in the results section. Since the adaption process implies a certain processing delay in each node, it is very important to reach a balance between the number of (periodical) adaptations and the processing time involved.

Each queue associated to a particular VO is characterized by its size, $QS(VO_i)_n$, which represents the number of packets stored in memory at a certain instant T_n. This size remains unchanged until a new event (arrival or departure of a packet) happens in T_{n+k}. The average queue occupation of this particular queue, $QO(VO_i)$, is calculated by the expression:

$$QO(VO_i) = \frac{\sum_{t=0}^{t=n} QS(o_i)_n \cdot (T_{n+k} - T_n)}{T_{n+k}}$$

It might seem desirable that the AWRR algorithm readapts weights as quickly as possible to peak rate variations of the traffic generation. Nevertheless, we cannot completely obviate historical patterns because otherwise those VOs that stop sending data for a short time would be instantly penalized. In order to allow the TDMA scheduler to tune the AWRR algorithm depending on the network requirements, two parameters α and β are defined, where α is associated to short-lived variations and β is associated to long-lived variations. We define the LastMean, $LM(VO_i)$, as the $QO(VO_i)$ obtained during the last time-window calculation and the HistoricalMean, $HM(VO_i)$, as the $QO(VO_i)$ averaged from the beginning. The TotalMean $TM(VO_i)$ is calculated by:

$$TM(VO_i) = \alpha \cdot LM(VO_i) + \beta \cdot HM(VO_i)\,; \qquad \{\, \alpha + \beta = 1 \,\}$$

The $TM(VO_i)$ is used by the AWRR algorithm to optimize the response of the TDMA scheduler. The mean TM, $\overline{TM}$, is calculated as:

$$\overline{TM} = \frac{\sum_{i=0}^{N} TM(VO_i)}{N}$$

The adjustment of new $W(VO_i)$ is proportional to the difference between each $TM(VO_i)$ and the $\overline{TM}$. That is, for those VOs with $TM(VO_i) > \overline{TM}$ their weight will be increased and viceversa for the opposite case. See lines 1 to 10 of algorithm 1. As we explained, the new $W(VO_i)$ of all VOs must always be maintained above (at least equal to) their predefined $MW(VO_i)$. If the AWRR needs to take away more units than permitted from VO_1 (it has already reached its minimum weight), the algorithm will get the proportional amount of units from the rest of VOs. See lines 13 to 25 of algorithm 1.

In this algorithm 1 we summarize all the details involved in the AWRR Scheduler. It covers one of the iterations to readapt VO weights.

Algorithm 1. AWRR Scheduler

```
1: for all $VO_I$ do
2:    /* Calculate the delta value to sum/rest to each $W(VO_i)$ */
3:    Delta = ( ($TM(VO_i) - \overline{TM}$) / $QS(VO_i)$ ) · $W(VO_i)$
4:    if $W(VO_i)$ + Delta >= $MW(VO_i)$ then
5:       $W(VO_i) = W(VO_i)$ + Delta
6:    else
7:       Rest = Rest + ( Delta – ($W(VO_i) - MW(VO_i)$))
8:       $W(VO_i) = MW(VO_i)$
9:    end if
10: end for
11: if Rest = 0 then
12:    finish
13: else
14:    while Rest > 0 do
15:       /* Calculate the delta value to be subtracted from each $W(VO_i)$ */
16:       Delta = Rest / NumVO (Not Minimum weight)
17:       if $W(VO_i)$ – Delta >= $MW(VO_i)$ then
18:          $W(VO_i) = W(VO_i)$ – Delta
19:          Rest = Rest – Delta
20:       else
21:          $W(VO_i) = MW(VO_i)$
22:          Rest = Rest – ($W(VO_i) - MW(VO_i)$)
23:       end if
24:    end while
25: end if
26: finish
```

4 Scenarios and Simulation Results

In order to quantify the aforementioned aspects we have particularized the wireless medium virtualisation problem for several scenarios.

The evaluation of the proposed scheduler has been developed within the NS2 environment [13], a C++ and TCL based discrete event simulator widely used in academic research. An implemented version is available at [14]. NS2 implements full protocol stacks and is able to simulate wired and wireless topologies using different transmission technologies. Typically, transport layer protocols, routing protocols, interface queues, and also link layer mechanisms can be configured. Moreover, propagation times between nodes are considered by the simulator. In NS2 network physical activities are translated to events that are enqueued and processed in the order of their scheduled occurrences.

4.1 Ad-Hoc Network Topology

The first scenario proposed to assess the benefits of the AWRR Scheduler is an Ad-Hoc network where a set of 4 nodes are located in a straight line topology (bus), so that transmissions consist of several hops among edges. The wireless technology used in this scenario is the standard 802.11. We consider that VOs can only send traffic during their TS, but can receive packets any time during the quantum.

Traffic generation is characterized by the inter-arrival time, λ, defined as a constant bit rate. That way, the analysis of the queue evolution is done just by the adaption of the weights by the AWRR scheduler and independently of the variations on the inter-arrival time by processes such as Poisson. All the packets transmitted have a constant size of 100 bytes.

Table 1 and 2 show the set of transmissions defined in the simulation and the evolution of the VOs in the communication network. We assume that the TSs and the active operators are perfectly synchronized in all nodes at the beginning of the simulation.

Table 1. Set of transmission flows

VO	Src Node	Dst Node	Start time	Finish Time	λ (ms)
1	0	3	20	1000	50
1	3	0	100	600	100
2	2	0	200	400	25
2	2	0	600	800	20
3	3	2	100	400	80
4	1	3	400	800	60
5	3	0	610	900	40

Table 2. Virtual Operator scheduled events

VO	Action	Time
3	Disappear	450
5	Appear	600

First, the benefits of the proposed tuning parameters to smooth the effects of the appearance of new flows and VOs are assessed. We evaluate the first flow of VO_1 (i.e. 3 hops) because it is the longest connection and the scheduled events of flows and VOs occur inside its duration time. Figure depicts the calculated average delay time (normalized per time unit) in several possible combinations: only the $HM(VO_i)$ is considered ($\alpha = 0$, $\beta = 1$); only the $LM(VO_i)$ is considered ($\alpha = 1$, $\beta = 0$); and the intermediate case ($\alpha = 0.5$, $\beta = 0.5$). The AWRR algorithm has been executed every 10 quantums, i.e. every 4 seconds.

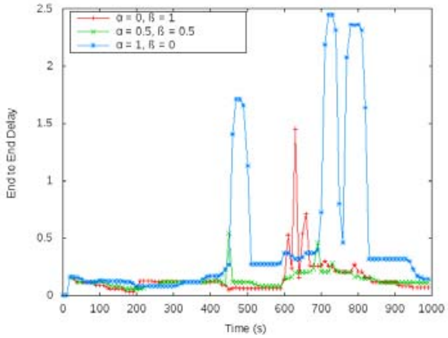


Fig. 2. End to end average delay for the comparison of the tuning parameters

As we can observe, the intermediate case (marked in the graph with *) is the one showing best performance, since extreme cases (marked in the graph with X and I) present more difficulties to adapt to changes and lead to congestion situations. If we only consider the $LM(VO_i)$ when a new flow belonging to a new transmitting VO appears (its $W(VO_i)$ was at $MW(VO_i)$), the queue utilization value will be suddenly very high and it will be granted by the adaption algorithm with a very large $W(VO_i)$, provoking congestion to the other VOs in the following re-adaptations. On the contrary, if we only consider the $HM(VO_i)$, the system will spend a lot of time to provide a large $W(VO_i)$ to new flows causing congestion and many packets losses.

Once the benefits of the tuning parameters have been exposed, the performance improvement for the intermediate case ($\alpha = 0.5$, $\beta = 0.5$) will be assessed. We can clearly see two different situations in the graph depicted in figure 3. Until second 600 the depicted flow is the one with the bigger bit rate so the AWRR scheduler reduces the delay compared to the classical RR case (marked in the graph with *). With the appearance of the flows associated to VO_2 and VO_4, which are characterized by a lower inter-arrival time, we can observe how the delay of VO_1 increases because the AWRR scheduler reduces $W(VO_1)$ and increases $W(VO_2)$ and $W(VO_4)$.

Focusing now on the adaption methods (i.e. packets sent and quantum rounds), after analyzing a set of simulations with different values for each one, the best results are displayed in figure 3. We can conclude that the one triggered by the quantum rounds (marked in the graph with |) behaves much better. At the beginning of the simulation only VO_1 is sending data, so the packet triggered method (marked in the graph with X) needs a long time to send the number of packets established as the threshold, and the adaption is performed very slowly, becoming inefficient. Moreover, in the second half of the simulation when a lot of packets are being sent, the adaption is performed too fast, which makes the process a bit unstable. We can observe in the graph two peaks for the adaption case triggered by the quantum rounds: they are caused by the congestion derived by variations in the transmission flows and the fixed time interval between adaptions.

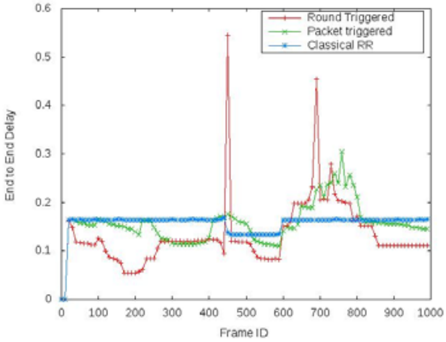


Fig. 3. End to end average delay for the comparison of the adaption methods

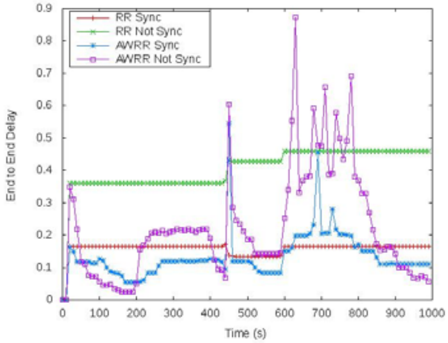


Fig. 4. End to end average delay for the synchronized and non-synchronized cases

Up to now we have assumed synchronization among all nodes. However, sometimes this situation can not be assumed. In figure 4 we show the average delay calculated for the same topology previously analyzed, but comparing the synchronized and non-synchronized transmission. As we could expect, the synchronized case behaves much better since packets can be forwarded directly from the source to the destination in the same time slot without intermediate stops. We can also observe that the AWRR scheduler (marked in the graph with *) has a better response compared to the classical RR scheduler (marked in the graph with).

4.2 Infrastructure Network Topology

The second scenario we have assessed consists in sending several video streams, each one belonging to a particular VO in an infrastructure based topology. The wireless technology chosen for sending the video frames has been the mobile extension of the IEEE 802.16 standard (802.16e, Mobile WiMAX). This technology provides a better solution in terms of bandwidth and coverage area than other wireless schemes such as 802.11. Since 802.16e is not implemented in the official NS2 release, the widely used NIST provided simulation patch [15] has been used.

Several video transmissions have been carried out by using the Evalvid tool [16] as TG, integrated within the NS2 network simulator. Evalvid generates the input source file from the information of video frames to be sent in our scenario in NS2, and also provides the tools to assess the quality of the video streams at the reception node.

The proposed network architecture is depicted in figure 5. We can observe the existence of a central video server in the picture, which sends and routes the video frames to the base stations. Since the requirements of each base station could be different depending on how many VOs are sending video streams at a time, the AWRR scheduler is applied individually in each base station.

Our research has been focused on the transmission of streaming video or Video on Demand (VoD). In order to reduce the jitter experimented by video frames [17], this type of video transmission assumes the existence of a buffer of some seconds at

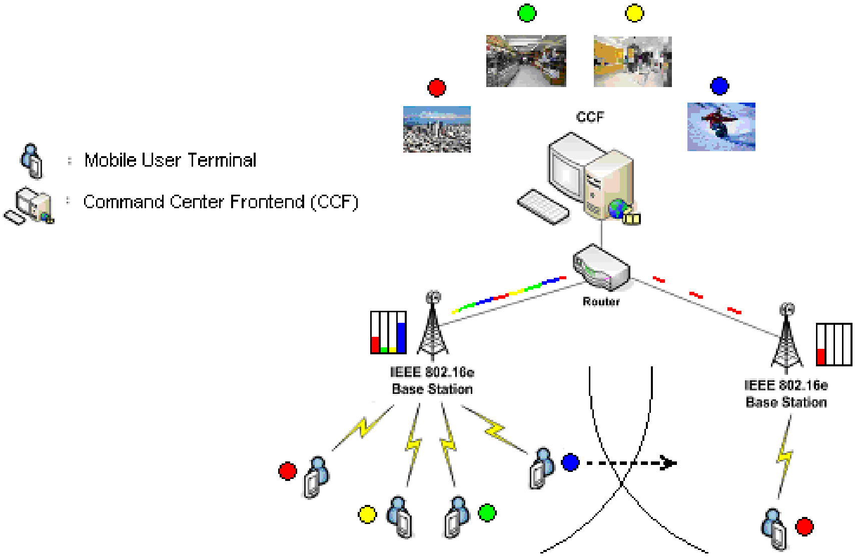

Mobile User Terminal
Command Center Frontend (CCF)
CCF
Router
IEEE 802.16e Base Station
IEEE 802.16e Base Station

Fig. 5. Network scheme for video transmission

the reception node. In this case the main constraint to overcome is to maintain data losses below the 5 percent recommended for such applications [17].

Four video samples in raw yuv format with a duration longer than three minutes and CIF resolution (352×288 pixels) are considered in our analysis. All the video files where compressed using the H.264/AVC [18] video codec for the transmission. The selection of the video samples is done by covering different levels of dynamism within the frames as we can observe in table 3. When we send a video with higher grade of movement and we do not want to lose quality, we need to increase the number of frames per second or reduce the Group of Pictures (GoP) so that the distance between two intra-frames (I frames) is shorter (increase the percentage of I frames in the coded video file). This fact implies the need of a higher bandwidth, and thus, much more packets to be sent.

Table 3. Transmitted video files

Video File	Level of Dynamism	Bit Rate
SecurityCamera1.yuv	Low	400 kbps
SecurityCamera2.yuv	Low	400 kbps
City.yuv	Medium	800 kbps
Ski.yuv	High	1200 kbps

The first case of analysis consist in the transmission of the four video files, each one belonging to a particular VO, with a 400 milliseconds quantum time and a queue size of 50 packets. These resources are enough for the transmission of videos with low grade of dynamism, but not for those with a higher level, what causes a queue overflow and some frame losses. The adaption is performed every 4 seconds.

Figure 6 – left shows the overall percentage of lost frames per video file depending on the TDMA scheduler used in one base station. As we can observe, the percentage of losses for the AWRR scheduler is much lower and therefore the quality of the videos will be better preserved. In this case the videos with greater grade of dynamism are granted with a larger weight, reducing the amount of lost packets without penalizing the rest of transmissions. Of course, if we would send three or less videos instead of four without reducing the number of VOs in the system, the percentage of losses for the AWRR Scheduler would be even lower.

Usually the scheduler will have to deal with dynamic scenarios where users move towards the radio coverage of another base station while they are receiving the video stream (handover). A user is able to request a new video or stop the one he is watching whenever he wants, so the video transmissions start and stop unexpectedly. Since we cannot plan when a client is going to require a handover or restart a transmission, the base stations cannot remove any of the VO queues permanently even if no video files are being transmitted by that operator. Figure 6 – right shows the percentage of lost packets for a dynamic scenario where users require handovers and transmissions begin randomly within the simulation time. Once again the AWRR results in a better performance. In the graph we can observe an increase in the percentage of lost frames using the AWRR scheduler. This occurs because when a VO starts a new flow after a while without transmitting anything, its $W(VO_i)$ will be at its minimum, $MW(VO_i)$. Many frames will get lost until the scheduler readapts the weights.

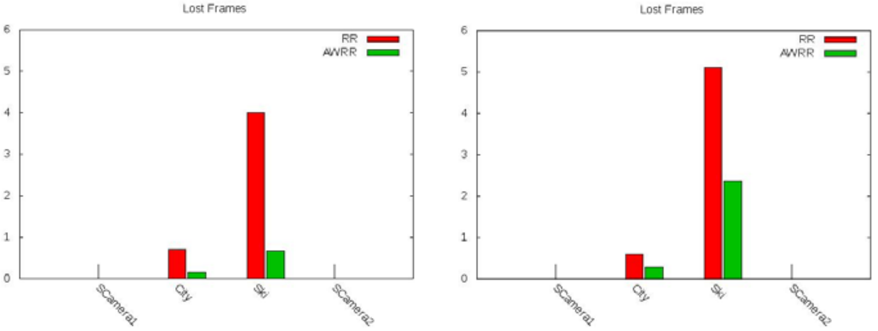


Fig. 6. Percentage of lost frames

5 Conclusions

The proliferation of new operators willing to offer services over physical substrates of others infrastructure providers makes network virtualization an important research field for the construction of the Future Internet. Virtualization of the wireless medium pursues the maximization of usage of a specific wireless physical resource by several VOs running services through the same wireless interface. This work has presented an AWRR algorithm that improves the average performance of a TDMA scheduler.

The benefits of the proposed algorithm have been assessed for two scenarios where the constraints and the requirements of the VOs were quite different. Results in both cases have been pretty promising since the performance and the QoS parameters monitored have been improved with respect to other static scheduling techniques.

As future work to be outlined, the adaption could be tackled from different points of analysis, i.e. the utilization of the channel and the average waiting time, so that a more exhaustive comparison could be carried out. Another future line is to enhance the adaption both introducing more complexity in the algorithm and the tuning parameters or trying to envisage future needs of the VOs according to new generation services and applications.

Acknowledgements

This work has been co-funded by the European Project 4WARD (FP7 Project reference: 216041), and the Future Internet Project, a Research Project from the Basque Government inside the Etortek Program.

References

1. Peterson, L., Shenker, S., Turner, J.: Overcoming the Internet impasse through Virtualization. In: ACM HotNets III (2004)
2. Feamster, N., Gao, L., Rexford, J.: How to lease the Internet in your spare time. Georgia Tech. Technical Report GT-CSS-06-10 (August 2006)
3. Carapinha, J., Jiménez, J.: Network Virtualization – a View from the Bottom. In: ACM SIGCOMM Workshop on Virtualized Infastructure Systems and Architectures (VISA), Barcelona, Spain (August 2009)
4. Hernando, G., Pérez, S., Cabero, J.M.: Mobility-Aware Distributed Embedding (MADE) of virtual networks. In: Future Network & Mobile Summit 2010, Florence, Italy (June 2010)
5. Lu, J., Turner, J.: Efficient Mapping of Virtual Networks onto a shared substrate. In: IEEE International Conference on Network Protocols (2006)
6. Sachs., J., Baucke, S.: Virtual radio: A framework for configurable radio networks. In: International Wireless Internet Conference (WICON), Maui, USA (2008)
7. Egi, N., Greenhalgh, A., Handley, M., Hoerdt, M., Huici, F., Mathy, L.: Towards High Performance Virtual Routers on Commodity Hardware. In: ACM CoNEXT, Madrid, Spain (December 2008)
8. GENI: Global Environment for Network Innovations: Technical document on wireless virtualization (September 15, 2006)
9. Round-Robin Scheduling, `http://en.wikipedia.org/wiki/Round-robin_scheduling`
10. Pérez, S., Cabero, J.M., Miguel, E.: Virtualization of the Wireless Medium: a Simulation-Based Study. In: 69th Vehicular Technology Conference: VTC 2009-Spring, Barcelona, Spain (April 2009)
11. Anastasi, G., De Stefano, E., Lenzini, L.: QoS provided by the IEEE 802.11 wireless LAN to advanced data applications: a simulation analysis. Wireless Networks 6(2), 99–108 (2000), ISSN:1022-0038
12. Chuah, C.N., Katz, R.H.: Characterizing packet audio streams from internet multimedia applications. In: ICC 2002 - IEEE International Conference and Communications (April 2002)
13. Network Simulator 2, NS2, official web page, `http://www.isi.edu/nsnam/ns/`
14. AWRR patch for NS2, `http://www.tecnalia.es/telecom-products.php`
15. NIST Wimax and MIH Module for NS2, `http://w3.antd.nist.gov/seamlessandsecure/`
16. Klaue, J., Rathke, B., Wolisz, A.: EvalVid - A Framework for Video Transmission and Quality Evaluation. In: 13th International Conference on Modelling Techniques and Tools for Computer Performance Evaluation
17. Szigeti, T., Hattingh, C.: Quality of serving design overview, `http://www.ciscopress.com/articles/article.asp?p=357102&seqNum=2`
18. Stockhammer, T., Hannuksela, M.M., Wiegand, T.: H.264/AVC in Wireless Environments. IEEE Transactions on Circuits and Systems for Video Technology 13(7), 657–673 (2003)

Robust Wireless Network Coding – An Overview

Marco Di Renzo[1], Lana Iwaza[1,2], Michel Kieffer[1],
Pierre Duhamel[1], and Khaldoun Al Agha[2]

[1] Laboratoire des Signaux et Systèmes, CNRS – SUPELEC – Univ. Paris–Sud 11
91192 Gif–sur–Yvette, Paris, France
{marco.direnzo,lana.iwaza,michel.kieffer,pierre.duhamel}@lss.supelec.fr
http://www.lss.supelec.fr
[2] Laboratoire de Recherche en Informatique, CNRS – Univ. Paris–Sud 11
91405 Orsay, Paris, France
alagha@lri.fr
http://www.lri.fr

Abstract. Network Coding (NC) has witnessed a tremendous upsurge in interest and activities in recent years, both in academia and industry. Indeed, since the pioneering publication of Ahlswede *et al.* in 2000, NC has rapidly emerged as a major research area in information theory due to its wide applicability to communication through real networks. The many contributions available in the literature to date, ranging from purely theoretical studies on fundamental limits to practical experimentations in real–world environments, offer a clear evidence that the shift in paradigm envisaged by NC might revolutionize the way we manage, operate, and understand the organization of networks. However, the principle of NC is not without its limitations. Initial studies on NC were mainly focused on lossless channels, which, however, might have limited applicability to a wireless context. As a matter of fact, in practical wireless environments, NC might be very susceptible to transmission errors caused by noise, fading, or interference. In particular, the algebraic operations accomplished by the intermediate nodes of the network introduce some packet dependencies in a way that the injection of even a *single* erroneous packet has the potential to corrupt *every* packet received by the destination nodes. Motivated by this consideration, recent research efforts have been devoted to the design of *robust* NC, with the main goal to circumvent the critical limitations of the NC paradigm in practical operating environments. In this paper, we aim at providing an overview of the most important and notable research directions in this emerging field.

Keywords: Network Information Flow, Network Coding, Error Control, Coding over Networks, Joint Network–Channel Decoding, Reliable Communications, Wireless Networks.

1 Introduction

Communication networks are designed to deliver information from source to destination nodes. The traditional way of delivering data employs paths for unicast connections and trees for multicast connections. When data is routed over

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 685–698, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

a unicast path, each intermediate node forwards the packets received over its incoming edges to its outgoing edges. While, in a multicast connection over a tree the intermediate nodes may duplicate packets and forward them to several outgoing edges. In other words, in today practical communication networks information delivery is accomplished through *routing*: network nodes simply store and forward data, and processing is only accomplished at the end nodes. Network Coding (NC) is a recent field in information theory that breaks with this assumption: instead of simply forwarding data, the intermediate nodes may recombine several input packets into one or several output packets. This way, NC allows the intermediate nodes to generate new packets by combining those received on their incoming edges. The potential advantages of NC over routing include resource (*e.g.*, bandwidth and power) efficiency, computational efficiency, and robustness to changes in the topology of the network [1].

Research on NC was initiated by the seminal paper [2], and has since then attracted significant interest from the research community. Many initial works on NC focused on establishing multicast connections. It was shown in [2] that the capacity of multicast networks (*i.e.*, the maximum number of packets that can be sent from the source to a set of terminals per time unit) can be achieved by coding within the network, *i.e.*, by allowing the mixing of data at the intermediate nodes of the network. A few years later, in [3] it was shown that, for multicast networks, linear coding at the intermediate nodes suffices to achieve the capacity limit, which is the max–flow from the source to each receiving node. In [4], the authors extended the results in [3] to arbitrary networks and introduced a very powerful algebraic framework for NC. The approach establishes a useful connection between a NC problem and the solution of certain systems of polynomial equations. In [5], the authors conceived a practical NC scheme without need of centralized knowledge of the network topology or of the encoding/decoding functions. The fundamental idea of [5] consists in including within each transmitted packet the global encoding vector along the edge. This way, these latter vectors, which are needed to decode the data received at any receiver, can be found in the arriving packets themselves. With the cost of a reasonable overhead, the approach can offer a totally decentralized solution to NC over networks. In [6], the authors capitalized on the analytical formulation of [4] and the practical scheme in [5] by proposing a distributed and fully randomized method to design the network codes. Moreover, it was shown in [6] that the network capacity can be achieved with probability exponentially approaching one with the code length. Finally, on a more practical side, Katti *et al.* conceived several solutions, *i.e.*, COPE, ANC, MIXIT, MORE, to efficiently exploit the NC paradigm over wireless networks [7]–[10].

However, besides the many potential advantages and applications of NC over classical routing (see, *e.g.*, [11], [12]), the NC principle is not without its drawbacks. A fundamental problem that NC needs to face with over lossy networks is the so–called *error control problem*: corrupted packets injected by some intermediate nodes might propagate through the network until the destination, and might render impossible to decode the original information. In contrast to routing, this problem is crucial in NC due to the algebraic operations performed by the internal nodes of the network. As a matter of fact, the mixing of packets within the network makes every packet flowing through it statistically dependent on other packets: even a single erroneous packet might affect the correct detection of all other packets. On the contrary, the same error in networks using just routing would affect only a single source–destination path. Broadly speaking, possible errors in NC might arise for three main reasons [13]: i) *erasures*, which lead to insufficiently received packets at the destination to solve the NC problem and retrieve the transmitted messages, ii) *errors*, which are due to using, for complexity and practical reasons, not powerful enough link–to–link error–correcting codes or are caused by the need to avoid a retransmission of all corrupted packets, and iii) the presence of intentional *jammers*, who might introduce erroneous packets at the application layer, which might be difficult to be recovered by the destination node. In such a context, the conventional approach to drop all erroneous packets detected at the physical layer, might be very sub–optimal for several reasons, *e.g.*, i) this may lead to insufficiently received packets for decoding and may be very spectrally inefficient, ii) even packets with errors could be a source of redundancy that may help the decoding process at the destination node, and iii) even though some bits are wrong, some parts of the packets are still error–free and could be exploited via some joint source–channel decoding methods to correct the wrong–bits.

In the light of all the above, robust NC is concerned with the design of efficient methods to design codes and decoding algorithms that are robust to all kinds of errors above, and can be decoded in a computationally efficient way. In this paper, we provide an overview of two important approaches to improve the reliability of network–coded data transmission over lossy networks: i) the design of error–correcting codes in projective spaces [14], and ii) the design of joint network–channel decoding schemes [15]. The first method moves from the key observation that in random linear NC the only property of the matrix containing the transmitted packets that is preserved is its row space. Thus, the information to be transmitted should be encoded in the choice of a subspace rather than in a specific matrix. On the other hand, the second method advocates a joint decoding of network and channel codes in order to fully exploit the spatial diversity and redundancy residing in both of them. Of course, both views are two sides of the same coin: they both aim at improving the performance and robustness of network–coded wireless architectures over lossy networks.

The reminder of this paper is organized as follows. In Section 2, the concept of linear NC is introduced in a formal way, and the fundamental algebraic tool introduced in [4] for its analysis is carefully described along with the concept of Random Linear Network Coding Channel (RLNCC) model widely adopted to describe the behavior of lossy networks. In Section 3 and Section 4, recent results on the design of codes in projective spaces and on the joint decoding of network and channel codes are summarized, respectively. Finally, Section 5 concludes the paper.

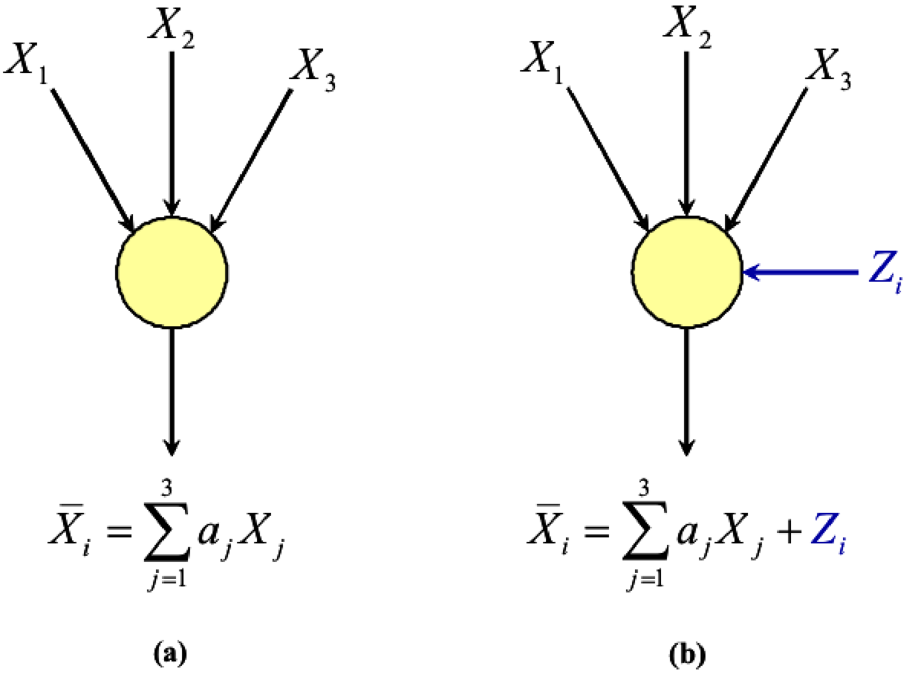

X_1
X_2
X_3
$\bar{X}_i = \sum_{j=1}^{3} a_j X_j$
(a)
X_1
X_2
X_3
Z_i
$\bar{X}_i = \sum_{j=1}^{3} a_j X_j + Z_i$
(b)

Fig. 1. Example of "injection packets" for a generic nodes of the network. (a) Error–free scenario. (b) Error–prone scenario. $\{a_j\}_{j=1}^{3}$ are the coefficients of the network code.

2 Fundamentals of Network Coding

Let us consider, for illustrative purposes, a point–to–point communication network with a single source node and a single destination node. Let us also assume, for the moment, that each link in the network transports free of errors a packet of M symbols in a given finite field $\mathbb{F}_q$. During each transmission, the source node sends n information vectors (*i.e.*, packets) $X_1, X_2, \ldots, X_n$, each one with size $1 \times M$. Whenever a node of the network (with the inclusion of the source node) has an opportunity for transmission, it produces an outgoing packet that is obtained as a random linear combination (with values over the field $\mathbb{F}_q$) of all incoming packets received until then. Each node of the network performs this operation until the destination node collects N packets $Y_1, Y_2, \ldots, Y_N$, from which it tries to infer the original data emitted by the source node, *i.e.*, $X_1, X_2, \ldots, X_n$.

Let us now cast the transmitted $X_1, X_2, \ldots, X_n$ and received $Y_1, Y_2, \ldots, Y_N$ packets into a compact matrix representation form. Let X be a $n \times M$ matrix whose rows are the vectors $X_1, X_2, \ldots, X_n$. Similarly, let Y be a $N \times M$ matrix whose rows are the vectors $Y_1, Y_2, \ldots, Y_N$. Owing to the assumption of linear operations performed by each node of the network, Y and X can be related by the following simple matrix expression:

$$Y = AX \tag{1}$$

where A is a $N \times n$ matrix that corresponds to the overall linear transformation applied by the network. The interested reader is kindly referred to [4, Sec. III] for further details about the algebraic model in (1). According to the above error–free model, it follows that the receiver can obtain the set of transmitted packets $X_1, X_2, \ldots, X_n$ from the set of received packets $Y_1, Y_2, \ldots, Y_N$ by simply solving the set of linear equations in (1).

Let us now remove the assumption of error–free transmission over the wireless links. A widely adopted channel model for NC is the so–called RLNCC model. It assumes that packet errors might occur in any link of the network and are modeled as "injection packets". In other words, a corrupted packet is modeled as the addition of an error packet to a genuine packet. According to this model, let us denote by Z_i the error packet applied at link $i \in \{1, 2, \ldots, L\}$, with L denoting the number of links of the network (see Fig. 1 for a simple example). By casting the L error packets into a $L \times M$ matrix denoted by Z, the signal received at the destination node can be re–written as follows:

$$Y = AX + BZ \tag{2}$$

where B is a $N \times L$ matrix that corresponds to the overall linear transformation applied, from the link they are injected to the destination node, to $Z_1, Z_2, \ldots, Z_L$. If $Z_i = 0$, there is no injected error to link i. Furthermore, if $Z_i = 0$ for all $i \in \{1, 2, \ldots, L\}$, then there are no corrupted packets in the network and (2) reduces to (1).

According to the above RLNCC model, the concepts of erasure, errors, and jamming can also be better clarified for NC. In particular: i) erasures happen when the rank of AX is smaller than the rank of X, and ii) errors and jamming happen when $Z_i \neq 0$ for some $i \in \{1, 2, \ldots, L\}$ [14].

3 Error–Correcting Codes in Projective Spaces

In this section, we summarize the main contributions on the analysis and design of error–correcting codes, introduce the concept of code design in projective spaces pioneering conceived in [14], and describe the latest developments in this research area.

The first landmark approaches to the design of error control codes for network–coded systems were presented in [16]–[18]. In those papers, the authors introduced the concept of *network error correction*, whose main idea is to design the network code so that it can be used for error correction. The underlying idea is to exploit the network code for protecting the messages transmitted through the network from distributed errors occurring over the individual links, which are not assumed to be error–free. Network error correction generalizes the usual link–to–link error correction methods adopted in conventional networks. Broadly speaking, the method introduced in [16]–[18] considers the design of a network code as part of an error control problem. Moving from the original idea of network error correction introduced in [16], many subsequent papers investigated that problem with the main aim of computing fundamental performance bounds, and propose code constructions and efficient decoding algorithms for network error–correcting codes. Notable examples along this line are [13], [19]–[21], and references therein.

A radical shift in paradigm on the design of error–correcting codes for random NC was introduced by Koetter and Kschischang in [14], who conceived the principle of coding for operator channels. This clever idea has originated an active field of research that is also known as error–correcting codes design in projective spaces (see, *e.g.*, [22]). The main idea behind [14] resides in recognizing that the natural transmission model of random NC consists of inputs and outputs that are subspaces of a given vector space. The interesting feature and main difference of the method introduced in [14], with respect to previous approaches available in the literature, is to be oblivious to both the network topology and the particular network code. In other words, the method introduced in [14] seeks to design an outer code that can be applied end–to–end without requiring any modifications on (or even the knowledge of) the underlying network code. The basic idea is to encode the information in the choice, at the transmitter, of a vector space (rather than a vector), and to design, at the receiver, a suitable algorithm to reconstruct the subspace sent by the transmitter in the presence of different kinds of errors.

3.1 How It Works

The theoretic motivation behind the design of error–correcting codes in projective spaces can be captured by using the RLNCC model introduced in Section 2. Let us consider, for ease of illustration, the channel model in (1). Since in random NC the matrix A of the overall linear transformation applied by the network is unknown, it follows that, even in the absence of errors, the only property of the transmitted packets that is kept invariant after propagation through the RLNCC model in (1) is the product AX, which is the row space of X. In other words, from the point of view of the destination node, any of the possible generating sets for the space AX are equivalent. As a consequence, the conventional link–to–link code design, which foresees the transmission of the information via a suitable design of X, needs to be modified and generalized to convey the information via the vector space spanned by the row space of X.

Mathematically speaking, the transmission (and so the encoding via sub–space selection) can be stated as follows. Let $\mathcal{P}_q(n)$ be the projective space of order[1] n over the finite field $\mathbb{F}_q$, which is defined as the set of all subspaces of the vector space $\mathbb{F}_q^n$. Let us consider a subspace code $\Omega \subseteq P_q(n)$, which is a non–empty set of subspaces of $P_q(n)$, with maximum dimension n. According to [14], the source node selects a subspace $V \in \Omega$ and transmits it over the RLNCC model as the matrix X in (1) and (2), and such that $V = \langle X \rangle$, with $\langle \cdot \rangle$ denoting the row space of X. The destination node receives Y and compute $U = \langle Y \rangle$, from which the transmitted subspace V can be inferred by using the minimum distance decoder

---

[1] According to Section 2, n is the number of packets injected, for each transmission, in the network by the source node.

as follows:

$$\hat{V} = \underset{V \in \Omega}{\arg\min} \left\{ d_S \left(V, U \right) \right\} \tag{3}$$

where $d_S(\cdot,\cdot)$ is the subspace distance defined as:

$$d_S \left(V, U \right) = \dim \left(V \right) + \dim \left(U \right) - 2 \dim \left(V \cap U \right) \tag{4}$$

and $\dim(\cdot)$ denotes the dimension of a vector space.

In particular, the minimum distance decoder in (3) guarantees perfect decoding capabilities, *i.e.*, $\hat{V} = V$, if $d_S(V, U) < d_S(\Omega)/2$, where $d_S(\Omega)$ is the minimum subspace distance of the subspace code Ω, *i.e.*:

$$d_S \left(\Omega \right) = \min_{\substack{V_1, V_2 \in \Omega \\ V_1 \neq V_2}} \left\{ d_S \left(V_1, V_2 \right) \right\} \tag{5}$$

with V_1 and V_2 being arbitrary subspaces in Ω.

3.2 Recent Developments

Besides introducing the principle of error–correcting codes in projective spaces in [14], the authors also introduced a Reed–Solomon–like construction and described a Sudan–style minimum–distance decoding algorithm for the new family of subspace codes. Furthermore, the class of constant–dimension codes was introduced and investigated. Soon after [14], several contributions appeared in the literature with the goal of generalizing and improving the original idea. Relevant results in this research area are [23]–[31]. In [23], the authors study optimal constant–dimension codes for their application to NC, and show that Steiner structures are optimal constant–dimension codes. Two Johnson–type bounds are also computed. In [24], several new codes and bounds for the subspace metric introduced in [14] are derived. In [25], a large class of constant–dimension subspace codes is investigated. It is shown that codes in that class can be easily constructed from rank–metric codes, while preserving their distance properties. Moreover, it is shown that minimum distance decoding of such subspace codes can be reformulated as a generalized decoding problem for rank–metric codes where partial information about the error is available. Furthermore, for the important family of maximum rank–distance codes known as Gabidulin codes, an efficient decoding algorithm is proposed. In [26], the authors construct many new constant–dimension codes with a larger number of codewords than previously known codes. In [28], the authors study bounds and code constructions for the family of codes in [14] targeting the correction of insertions/deletions. In [29], the authors analyze the geometrical properties of rank–metric codes. They derive upper and lower bounds on the minimum cardinality of a code with a given rank covering radius and show that the proposed geometrical properties and bounds can be significant to the design, decoding, and performance analysis of rank–metric codes. In [22], a novel multilevel coding approach to construct codes in the projective space is presented. The method makes usage of four tools: an appropriate constant–weight code, the reduced row echelon form of a linear subspace, the Ferrers diagram related to this echelon form, and rank–metric codes related to the Ferrers diagram. The authors show that the codes proposed in [14] are a special case of the proposed family of codes. In [30], the error correction problem in both coherent and non–coherent NC is considered under an adversarial model. In particular, as far as non–coherent NC is concerned, the authors introduce a different metric with respect to [14], and prove that it yields a measure of code performance that is more precise, when a non–constant–dimension code is used, than [14]. The new metric is called injection metric. In [27], the authors introduce a Gilbert–Varshamov bound for the codes constructed in [30] according to the definition of injection metric. Moreover, the construction framework in [22] is exploited to obtain new non–constant–dimension codes, which are shown to contain a large number of codewords than comparable codes designed for the subspace metric. Finally, in [31] the authors address the very important problem of understanding if the codes introduced in [14] are feasible and suitable for hardware implementations. They show that the construction of these codes over small fields and limited error–correcting capabilities is not only feasible, but the resulting codes can achieve a high throughput.

4 Joint Network–Channel Decoding

In this section, we provide an overview of a slight different approach to improve the reliability of network–coded wireless architectures. The main idea consists in taking a cross–layer approach and leveraging technologies from the physical and network layers to combat the dominant impairment for an error–free delivery of information over wireless networks, *i.e.*, the channel fading. Of particular interest in the research community is the joint treatment of network and channel coding for improving the end–to–end performance and exploiting in an optimal way the spatial diversity and redundancy in both codes. This research field is motivated by recent results, which have clearly highlighted the fragility of a disjoint design of network and channel coding, as well as network and source coding [32]. By studying some canonical networks, it has been shown that source–channel separation may still hold for some networks, but source–network separation and channel–network separation usually break. Hence, although source coding and channel coding may still be treated separately in some network scenarios, separating routing (or more in general NC) from source or channel coding could fail to bring the desired end–to–end optimality. Furthermore, an end–to–end code design is advocated in [32] as well, where compression, channel coding, and NC/routing might not be separable functions in generic networks. Finally, in [33] it has also been shown that, even though for some networks the separation condition does not break optimality, a separate design of, *e.g.*, source and network codes may yield a higher cost (*e.g.*, may require more power or bandwidth) than their joint optimization.

The application of a joint treatment of network and channel coding finds an important application in lossy networks. As opposite to wireline networks, where it is usually considered that the lower layers deliver error–free or erasure–based links with the help of channel coding, in lossy networks the links are assumed to be error–prone. The principle of a joint design of network and channel codes resides in the exploitation of the redundancy of the network code to help the channel code for a better error protection. In other words, instead of guaranteeing the error–free transmission for each point–to–point link, one is only interested in guaranteeing error–free decoding at the destination nodes. These latter nodes have to decode the data using the input from all incoming links. If they have more than one incoming link, error–free decoding can be possible even if error–free decoding of the point–to–point links is not possible. So, joint network–channel decoding is useful, if the network code contains redundancy. The first practical application of this concept to relay networks is due to Hausl *et al.*, who conceived iterative network and channel decoding methods for the two–way and the multiple–access relay channels in [15] and [34], respectively. The results in these latter papers have evidenced that some performance improvements can be obtained by jointly decoding network and channel codes.

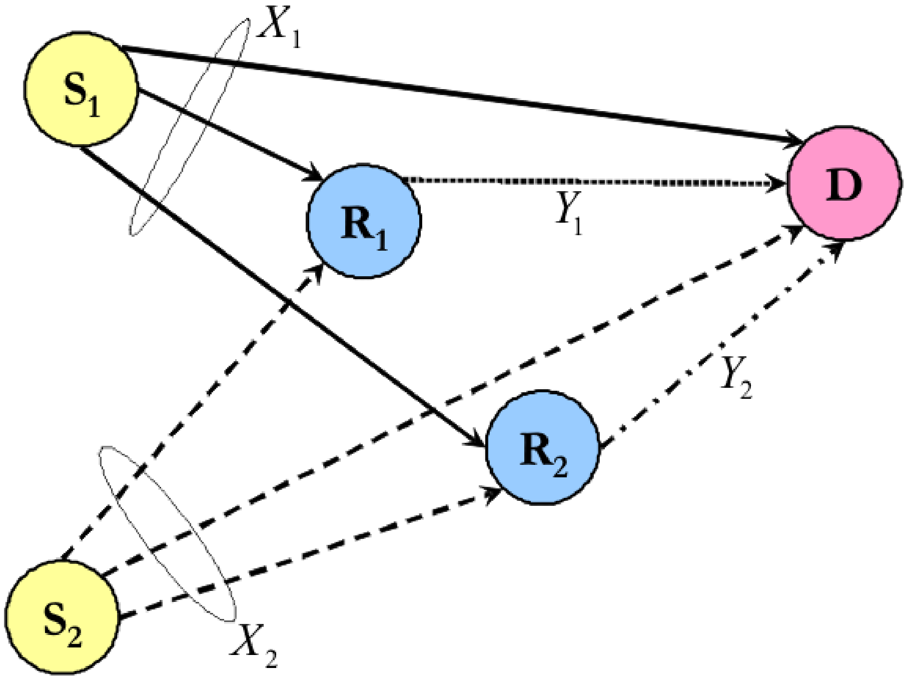


Fig. 2. Example of a two–source and two–relay network topology. Lines with different styles represent the transmission over orthogonal channels to avoid mutual interference.

4.1 Understanding Joint Network–Channel Decoding

Let us provide a simple example for understanding the rationale behind the joint treatment of network and channel coding. Let us consider, *e.g.*, a simple two–source and two–relay topology as shown in Fig. 2. We emphasize here that the conclusions drawn for the simple scheme in Fig. 2 can be extended to the general network topology described in Section 2. However, due to space constraints, this generalization is omitted in this paper. In Fig. 2, two sources S_1 and S_2 transmit two independent packets, of M symbols each, X_1 and X_2 to a common destination node D with the help of two relay nodes R_1 and R_2, respectively. Let us assume, for the sake of illustration, but without loss of generality, that all links are lossless, and that all communications take place over orthogonal channels such that mutual interferences can be neglected. Accordingly, the destination node will receive four packets from which it wants to infer the information messages, U_1 and U_2, emitted by the sources.

Let us assume that both packets X_1 and X_2 are channel–coded versions of the information messages U_1 and U_2 (of $\tilde{M}$ symbols each) actually produced by the sources S_1 and S_2, respectively. We assume general non–binary channel encoding over the field $\mathbb{F}_q$, as follows:

$$\begin{cases} X_1 = U_1 G_1 \\ X_2 = U_2 G_2 \end{cases} \tag{6}$$

where G_1 and G_2 are the $\tilde{M} \times M$ generator matrices describing the encoding at the source node S_1 and S_2, respectively.

By assuming error–free links, the relays R_1 and R_2 will ideally be able to retrieve[2] and to re–encode the messages U_1 and U_2 by performing network and channel coding. For illustrative purposes, let us consider the channel– and network–coded packets emitted by the relays as follows:

$$\begin{cases} Y_1 = a_{11} U_1 G_{11} + a_{12} U_2 G_{12} \\ Y_2 = a_{21} U_1 G_{21} + a_{22} U_2 G_{22} \end{cases} \tag{7}$$

where $\{a_{ij}\}_{i,j=1}^2$ are the coefficients of the network code and $\{G_{ij}\}_{i,j=1}^2$ the generator matrices for error protection.

Accordingly to (6) and (7), the destination node D receives four packets X_1, X_2, Y_1, and Y_2 from which it tries to retrieve the transmitted messages U_1 and U_2. By using a matrix notation, the following end–to–end equations can be obtained:

$$\begin{bmatrix} X_1 \\ X_2 \\ Y_1 \\ Y_2 \end{bmatrix} = \underbrace{\begin{bmatrix} G_1 & 0 \\ 0 & G_2 \\ a_{11} G_{11} & a_{12} G_{12} \\ a_{21} G_{21} & a_{22} G_{22} \end{bmatrix}}_{G_{\text{joint}}} \begin{bmatrix} U_1 \\ U_2 \end{bmatrix} \tag{8}$$

---

[2] The relays must know G_1 and G_2 and the related parity check matrices for decoding the individual links.

where G_{joint} can be seen as the generator matrix of a joint network–channel code that includes both network and channel coding operations.

The result in (8) clearly highlights that network and channel codes can be regarded, from an end–to–end point of view, as a single integrated code with generator matrix G_{joint}. Accordingly, the messages U_1 and U_2 could be decoded at the destination node by representing the integrated code in (8) by a factor graph and using some iterative decoding methods. This way, network and channel decoding can be performed jointly, by enabling the exchanging of information within and across the received packets to better exploit the redundancy of the network code and achieve some performance improvements. On the contrary, separate network and channel decoding foresee, in general, to exchange the information only within individual packets. A specific iterative decoding algorithm introduced in [35] for the simple network shown in Fig. 2 has clearly evidenced the potential gain of a joint decoding approach.

4.2 Recent Results

Moving from the basic idea in [15] and [34], various studies about the performance improvement of joint network and channel decoding are available in the literature. Most of these studies have the main objective to analyze the effectiveness of such a joint decoding design for the robust and reliable operation of network–coded wireless architectures over lossy networks and to overcome some initial assumptions retained in, *e.g.*, [15]. For example, in [15] ideal error–correcting codes are assumed for the source–to–relay channels, which results in having error–free communication over these links, as well as in introducing a diversity loss since the local channel code blocks the whole frame if just a single bit is erroneous (see, *e.g.*, [36], [37]). Some examples of recent research results addressing the exploitation and the benefits of a joint network–channel code design and decoding can be found in [38]–[48].

5 Concluding Remarks

In this paper, we have provided an overview of two important research fields for the robust design of network–coded wireless architectures over lossy networks: error–correcting code design in projective spaces and joint network–channel iterative decoding. We have clearly shown that both research fields are receiving an upsurge of interest in the research community. However, research in both fields is still at its infancy, and fundamental and open issues need to be still addressed for their practical and effective application to distributed wireless networks.

Acknowledgment

This work is supported by the research projects “New Communications with Network Coding (N2C)” funded by DIGITEO, and “JNCD4CoopNets” funded by CNRS - GDR 720 ISIS.

References

1. Ho, T., Koetter, R., Medard, M., Karger, D.R., Effros, M.: The benefits of coding over routing in a randomized setting. In: IEEE Int. Symposium Inform. Theory, p. 442 (June/July 2003)
2. Ahlswede, R., Cai, N., Li, S.-Y.R., Yeung, R.W.: Network information flow. IEEE Trans. Inform. Theory 46(4), 1204–1216 (2000)
3. Li, S.-Y.R., Yeung, R.W., Cai, N.: Linear network coding. IEEE Trans. Inform. Theory 49(2), 371–381 (2003)
4. Koetter, R., Medard, M.: An algebraic approach to network coding. IEEE/ACM Trans. Networking 11(5), 782–795 (2003)
5. Chou, P.A., Wu, Y., Jain, K.: Practical network coding. In: Allerton Conf. Commun. Control, Computing (October 2003)
6. Ho, T., Koetter, R., Medard, M., Karger, D.R., Effros, M., Shi, J., Leong, B.: A random linear network coding approach to multicast. IEEE Trans. Inform. Theory 52(10), 4413–4430 (2006)
7. Katti, S., Gollakota, S., Katabi, D.: Embracing wireless interference: Analog network coding. In: ACM SIGCOMM, pp. 397–408 (August 2007)
8. Katti, S., Katabi, D.: MIXIT: The network meets the wireless channel. In: ACM HotNets (November 2007)
9. Katti, S., Katabi, D., Balakrishnan, H., Medard, M.: Symbol–level network coding for wireless mesh networks. In: ACM SIGCOMM, pp. 401–412 (October 2008)
10. Katti, S., Rahul, H., Hu, W., Katabi, D., Medard, M., Crowcroft, J.: XORs in the air: Practical wireless network coding. IEEE/ACM Trans. Networking 16(3), 497–510 (2008)
11. Fragouli, C., Soljanin, E.: Network Coding Fundamentals 2(1) (2007)
12. Fragouli, C., Soljanin, E.: Network Coding Applications 2(2) (2007)
13. Zhang, Z.: Linear network error correction codes in packet networks. IEEE Trans. Inform. Theory 54(1), 209–218 (2008)
14. Koetter, R., Kschischang, F.R.: Coding for errors and erasures in random network coding. IEEE Trans. Inform. Theory 54(8), 3579–3591 (2008)
15. Hausl, C., Hagenauer, J.: Iterative network and channel decoding for the two–way relay channel. In: IEEE Int. Commun. Conf., pp. 1568–1573 (June 2006)
16. Cai, N., Yeung, R.W.: Network coding and error correction. In: IEEE Inform. Theory Workshop, pp. 119–122 (October 2002)
17. Yeung, R.W., Cai, N.: Network error correction, part I: Basic concepts and upper bounds. Commun. Information Systems 6(1), 19–36 (2006)
18. Cai, N., Yeung, R.W.: Network error correction, part II: Lower bounds. Commun. Information Systems 6(1), 37–54 (2006)
19. Matsumoto, R.: Construction algorithm for network error–correcting codes attaining the singleton bound. IEICE Trans. Fundamentals E90–A(9), 1–7 (2007)
20. Jaggi, S., Langberg, M., Katti, S., Ho, T., Katabi, D., Medard, M., Effros, M.: Resilient network coding in the presence of byzantine adversaries. IEEE Trans. Inform. Theory 54(6), 2596–2603 (2008)
21. Balli, H., Yan, X., Zhang, Z.: On randomized linear network codes and their error correction capabilities. IEEE Trans. Inform. Theory 55(7), 3148–3160 (2009)
22. Etzion, T., Silberstein, N.: Error–correcting codes in projective spaces via rank–metric codes and Ferrers diagrams. IEEE Trans. Inform. Theory 55(7), 2909–2919 (2009)

23. Xia, S.-T., Fu, F.-W.: Johnson type bounds on constant dimension codes. Designs, Codes, and Cryptography 50(2), 163–172 (2008)
24. Gabidulin, E.M., Bossert, M.: Codes for network coding. In: IEEE Int. Symposium Inform. Theory, pp. 867–870 (July 2008)
25. Silva, D., Kschischang, F.R., Koetter, R.: A rank–metric approach to error control in random network coding. IEEE Trans. Inform. Theory 54(9), 3951–3967 (2008)
26. Kohnert, A., Kurz, S.: Construction of large constant dimension codes with a prescribed minimum distance. LNCS, pp. 31–42. Springer, Heidelberg (December 2008)
27. Khaleghi, A., Kschischang, F.R.: Projective space codes for the injection metric, arXiv.org (April 2009), `http://arxiv.org/PS_cache/arxiv/pdf/0904/0904.0813v2.pdf`
28. Ahlswede, R., Aydinian, H.: On error control codes for radom network coding. In: IEEE Int. Workshop Network Coding Theory and Applications, pp. 68–73 (June 2009)
29. Gadouleau, M., Yan, Z.: Bounds on covering codes with the rank metric, arXiv.org (June 2009), `http://arxiv.org/PS_cache/arxiv/pdf/0809/0809.2968v2.pdf`
30. Silva, D., Kschischang, F.R.: On metrics for error correction in network coding, arXiv.org (August 2009), `http://arxiv.org/PS_cache/arxiv/pdf/0805/0805.3824v4.pdf`
31. Chen, N., Gadouleau, M., Yan, Z.: Rank metric decoder architectures for noncoherent error control in random network coding. In: IEEE Workshop Sig. Process. Systems (October 2009)
32. Effros, M., Medard, M., Ho, T., Ray, S., Karger, D., Koetter, R.: Linear network codes: A unified framework for source, channel and network coding. In: DIMACS Workshop Network Information Theory (March 2003)
33. Lee, A., Medard, M., Haigh, K., Gowan, S., Rubel, P.: Minimum–cost sub–graphs for joint distributed source and network coding. In: IEEE Workshop Network Coding, Theory and Applications (January 2007)
34. Hausl, C., Dupraz, P.: Joint network–channel coding for the multiple–access relay channel. In: IEEE Commun. Society on Sensor and Ad Hoc Commun. and Networks, pp. 817–822 (September 2006)
35. Guo, Z., Huang, J., Wang, B., Cui, J.-H., Zhou, S., Willett, P.: A practical joint network–channel coding scheme for reliable communication in wireless networks. In: ACM Int. Symposium on Mobile Ad Hoc Networking and Computing, pp. 279–288 (May 2009)
36. Xiao, L., Fuja, T.E., Kliewer, J., Costello, D.: A network coding approach to cooperative diversity. IEEE Trans. Inform. Theory 53(10), 3714–3722 (2007)
37. Al–Habian, G., Ghrayeb, A., Hasna, M.: Controlling error propagation in network–coded cooperative wireless networks. In: IEEE Int. Commun. Conf., pp. 1–6 (June 2009)
38. Bao, X., Li, J.: A unified channel–network coding treatment for user cooperation in wireless ad–hoc networks. In: IEEE Int. Symposium Inform. Theory, pp. 202–206 (July 2006)
39. Gowaikar, R., Dana, A.F., Hassibi, B., Effros, M.: A practical scheme for wireless network operation. IEEE Trans. Commun. 55(3), 463–476 (2007)
40. Zhang, S., Zhu, Y., Liew, S.C., Letaief, K.B.: Joint design of network coding and channel decoding for wireless networks. In: IEEE Wireless Commun. Conf., pp. 779–784 (March 2007)

41. Nguyen, H.T., Nguyen, H.H., Le–Ngoc, T.: A joint network–channel coding scheme for relay–based communications. In: IEEE Canadian Conf. Electrical and Computer Engineering, pp. 904–907 (April 2007)
42. Yang, S., Koetter, R.: Network coding over a noisy relay: A belief propagation approach. In: IEEE Int. Symposium Inform. Theory, pp. 801–804 (June 2007)
43. Kliewer, J., Dikaliotis, T., Ho, T.: On the performance of joint and separate channel and network coding in wireless fading networks. In: IEEE Workshop Inform. Theory for Wireless Networks, pp. 1–5 (July 2007)
44. Thobaben, R.: Joint network/channel coding for multi–user hybrid–ARQ. In: Int. ITG Conf. Source and Channel Coding, pp. 1–6 (January 2008)
45. Xu, X., Flanagan, M.F., Goertz, N.: A shared–relay cooperative diversity scheme based on joint channel and network coding in the multiple access channel. In: IEEE Int. Symposium Turbo Codes and Related Topics, pp. 243–248 (September 2008)
46. Bing, D., Jun, Z.: Design and optimization of joint network–channel LDPC code for wireless cooperative communications. In: IEEE Singapore Int. Conf. Commun. Systems, pp. 1625–1629 (November 2008)
47. Li, Q., Ting, S.H., Ho, C.K.: Joint network and channel coding for wireless networks. In: IEEE Conf. Sensor, Mesh and Ad Hoc Communications and Networks, pp. 1–6 (June 2009)
48. Li, Y., Song, G., Wang, L.: Design of joint network–low density parity check codes based on the EXIT charts. IEEE Commun. Lett. 13(8), 600–602 (2009)

Localization in Real GSM Network with Fingerprinting Utilization

Jozef Benikovsky, Peter Brida, and Juraj Machaj

University of Zilina, Faculty of Electrical Engineering,
Department of Telecommunications and Multimedia, Univerzitna 1, 010 26 Zilina, Slovakia
{jozef.benikovsky,peter.brida,juraj.machaj}@fel.uniza.sk

Abstract. This paper attempts to present current state in the area of user localization in cellular networks and shows custom solution for positioning using pocket computer and fingerprint method also known as fingerprinting. It operates in Global System for Mobile communications (GSM) network, although fingerprinting is also applicable in other wireless networks, such as Universal Mobile Telecommunications System (UMTS), Bluetooth or 802.11. Implementation is explained and it is compared to existing solutions. The performance of the system is evaluated for various scenarios by statistical characteristics and Circular Error Probability (CEP). The scenarios are proposed from observation of various parameters that influence the localization accuracy.

Keywords: Localization, Positioning, GSM, Fingerprinting method, Circular error probability.

1 Introduction

Location based services (LBS) attract more subscribers every year and number of them is expected to significantly grow over next years [1]. Therefore technologies that provide means to localize devices in unknown environments are interesting for research in order to provide faster, more accurate and generally better results for users.

The only currently operational global navigation system is Global Positioning System (GPS), which provides very good results. The problem with GPS is that users are required to buy new device (GPS receiver) or they have to buy high-end cell phone which offers embedded GPS receiver. Other problem is that GPS basically communicates in one way from satellite to user and other infrastructure is necessary when user needs to transmit some data. To overcome these issues, localization by means of GSM networks is taken into consideration, because GSM is the most used mobile technology with about 80% market share [2] (see Fig. 1) and provides communication between user and network operator as well as communication between users themselves.

Presently used localization methods are based on observation of miscellaneous signal parameters. Methods used in cellular networks are Cell Identification (Cell ID), Received Signal Strength (RSS), Angle of Arrival (AoA), Time of Arrival (ToA) and Time Difference of Arrival (TDoA) [3], [4] and [5]. The research of many specialists has been focused on RSS method [6], [7], [8], [9], [10], [11] which can be then processed using Trilateration technique [12], [13] or Fingerprinting technique [8], [9] and

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 699–709, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

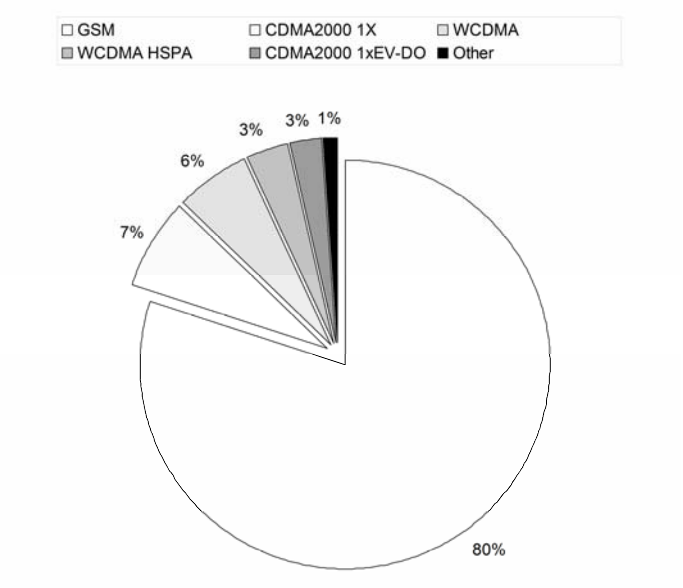


Fig. 1. Present market share of individual mobile technologies

[14]. Fingerprinting seems to be most accurate and affordable technique as it is suitable for Non Line-of-Sight (NLoS) environments as well as it is more immune to multipath than trilateration.

Our fingerprinting solution is based on received signal strength information. Generally, the RSS collection can be performed by either measurement in a real environment or prediction as described in [15]. In first case, it is very time consuming operation, but it is more precise, because real RSS information is used. In the latter case, prediction of RSS is more comfortable, but the data highly depend on a quality of map model of given environment. There is a compromise between the demanding effort and accuracy in [8].

This paper examines the accuracy of positioning system based on the proposed fingerprinting positioning system within a GSM network. Here we focus on an impact of different environments on positioning accuracy. The positioning accuracy is evaluated by median and circular error probability.

The system utilizes GPS coordinates as a reference position during radio map creation. Hence, advantage of the system consists in the fact that results of mobile positioning are presented in WGS-84 (World Geodetic System) and are compatible with GPS and maps based on WGS-84. The radio map is created automatically. The process of map creation is initialized and finalized by a device which performs measurements themselves. GSM and GPS data are measured during this process. When all desired data are measured, they are sent to the server. Some similar systems exist, but they are not based on GPS system [9]. In that case, reference points are marked manually in the map. The other way lies in association of reference points with fixed points, e.g. building, crossing, street, etc. Finally, the most important advantage is that the location system is independent on a network operator. The system only utilizes signals from a network operator.

The rest of the paper is structured as follows. Section 2 introduces fingerprinting phases, which are offline and online phase as well as explains basic GSM infrastructure and integration of fingerprinting into GSM environment. In Section 3, architecture of implemented positioning system is presented. Section 4 introduces experimental scenarios and experiments carried out in this study. In Section 5, the experimental results are presented and discussed. Section 6 concludes the paper and suggests some future studies.

2 Fingerprinting

The fingerprinting method relies on a uniqueness of radio fingerprints in a similar way than forensic science does with human fingerprints. The radio fingerprints are vectors of miscellaneous radio signal parameters such as received signal strength, timing advance or angles. These vectors are coupled with position coordinates and altogether form a database of well known spots, where these parameters are known. Fingerprinting has two phases, so-called offline and online phase, which are described in following sections.

2.1 Offline Phase

The offline phase is a process of radio fingerprint collection at some area and their load into database. For purpose of this work, Cell Identity (CID), Base Station Identification Code (BSIC), Broadcast Control Channel (BCCH) were measured in order to

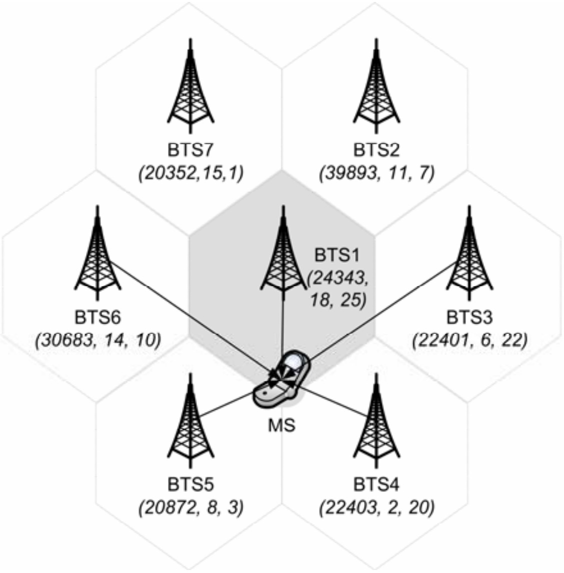


Fig. 2. Sample GSM environment with seven base transceiver stations (*BTS1-BTS7*) and one mobile station (*MS*). Base station identifiers (*the triple in parenthesis under BTS name*) are written in the following order (CID, BSIC and BCCH).

identify Base Transceiver Station, as shown in Fig. 2. At every spot, Received Signal Level (RxLev) of serving and neighbor cells was measured together with geographical coordinates such as latitude, longitude and altitude.

Fig. 2 displays Mobile Station (MS) surrounded by seven Base Transceiver Stations (BTS). The BTS1 is called serving BTS and the other ones (BTS2-BTS7) are called neighbor BTS. MS detects and measures signals from BTS1 and BTS3-BTS6. RxLev from these BTSs then form fingerprint vector. Each BTS is uniquely identified by aforementioned parameters CID, BSIC and BCCH.

2.2 Online Phase

The online phase is process of position estimation using radio fingerprint measured at unknown spot. The fingerprint is then compared to records in the database and by means of correlation the closest matching vector is found. For purpose of this work, Euclidean distance between individual vectors was measured. The closest matching vector is then treated as position estimation. This approach is called Nearest Neighbor (NN) and is the easiest and most common algorithm. Other techniques like K-Nearest Neighbor averaging (KNN), Smallest M-vertex Polygon (SMP), neural networks or Bayesian modeling could have been used as well [16].

3 Architecture of Localization System

Entire system uses fingerprint database as well as central computation server, as shown in Fig. 3. It is designed in service-oriented architecture, which is usable by service providers, such as GSM operators. The system structure allows easy implementation of changes, central maintenance and further optimization of accuracy and performance. It is usable by multiple users, which is one of the basic requirements for a network service.

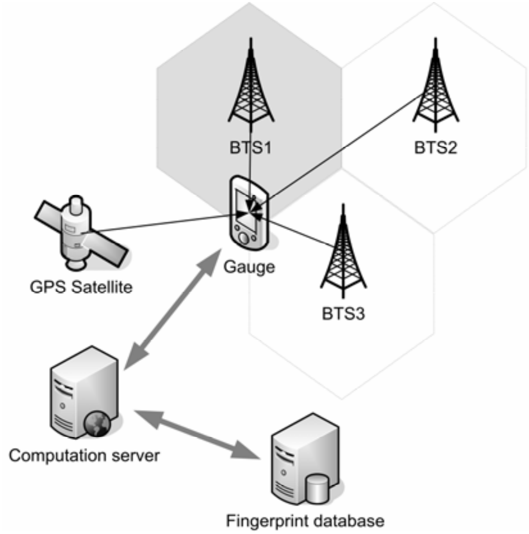


Fig. 3. Architecture of localization system

Gauge is a device that is able to measure necessary data from GSM network. In order to load database over offline phase, it has to be able to measure “precise” position, what is handled by integrated GPS receiver. For purpose of this work, pocket computer HP iPAQ hw6515d with Microsoft® Windows CE® 4.21 and Microsoft® .NET Compact Framework 2.0 were used.

Computation server contains web services that calculate estimated position using fingerprint vector from gauge, fingerprint database and NN algorithm. Furthermore, it also allows visualizing data stored in database utilizing Google Maps™ API.

Fingerprint database stores fingerprint vectors in a way that allows quick data retrieval. Oracle® Express database is utilized for this purpose.

3.1 Localization Algorithm

At first, *measurement* of GSM signals is done. Signal levels of adjacent BTSs and identifiers of these stations are detected. Then the radio map *database lookup* is made and set of interesting spots from database is returned. At third phase, Euclidean *metric calculation* is performed for every interesting spot and the nearest one is chosen as a position match. This is the simplest version of algorithm called NN. KNN, SMP or other techniques could have been used as stated above.

Lookup phase introduces optimization to localization process. After measurement is done, database is queried only for interesting spots, where at least one BS identifier matches current measurement. This reduces cardinality of returned set and speeds up metric calculation and position match processes. Increased performance allows doing more position estimations per time unit.

3.2 Localization Error

The localization error is calculated as a distance between estimated position **E** and reference position **R** measured by GPS. These two points are located on the surface of WGS-84 ellipsoid and difference in the altitudes can be neglected, because all measurements were performed at plain surface. Let γ be an angle between vectors that originate from centre of ellipsoid and head towards **E** and **R**. Let $R(\delta)$ be a function that calculates radius of Earth ellipsoid at geodetic latitude δ. Let lat_E and lat_R be the geodetic latitudes at point **E** or **R** respectively. Then the distance Δ between **E** and **R**, which represents localization error, is calculated as

$$\Delta = 0.5\gamma(R(lat_E) + R(lat_R)). \tag{1}$$

The equation basically calculates length of an arc located on the surface of sphere with radius of mean value between $R(lat_E)$ and $R(lat_R)$. The length is accurate enough for further calculations.

4 Experimental Setup

There were extensive experiments done in outdoor environment. All data were measured in the GSM network. The measurements were performed in three different scenarios by means of above described positioning service. The scenarios differ in environments where experiments were performed:

- scenario 1 - open area, at the edge of the Zilina city, with few movable reflectors (pedestrians, cars) and few buildings,
- scenario 2 - open area, rural part of the Zilina city with not many movable reflectors (pedestrians, cars) and many small houses,
- scenario 3 - urban area, Zilina city centre, with many movable reflectors (pedestrians, cars) as well as many building with various heights.

Database (*offline phase*) was created from received signal levels of the serving cell and up to six neighbor cells. Number of neighbor cells varied and six cells were not always available due to weak received signal. The measurements were performed with above mentioned pocket computer. The device moved at the speed of a pedestrian and it varied from 2 to 3 km/h. Samples were measured once per second. Measurements have been performed at about 2000 spots and carried out almost 14000 measurements per single scenario.

In the phase of localization (*online phase*), ten measurements were taken at 10 different spots for each scenario giving altogether 300 measurements and localization error was calculated for all of them. Then the average of the 10 localization errors was calculated for each spot and resulted in approximate localization error for certain spot. All ten approximate localization errors (for all ten spots) were then used to calculate statistical characteristics, such as median or Circular Error Probability (CEP), for all individual scenarios.

The three environments were purposely chosen because of their different properties. The areas have significantly different signal propagation conditions due to a various numbers of reflectors. Especially movable reflectors have unpredictable impact. For example, reflectors (cars and pedestrians) could have been at the point during process of map creation but not in the phase of localization. This phenomenon has the main impact on the positioning accuracy. The static reflectors should not have significant impact. Therefore it can be said that performance of localization service was validated in the representative samples of environment. The density of spots in database was same for all scenarios, i.e. distance between adjacent spots was approximately 2 meters. The number of used BTSs was no more than seven in all scenarios, but particular BTSs were different. The experiment was implemented in real GSM network which operates in the 900 MHz band.

The reference coordinates of MS position were obtained by means of GPS receiver in these experiments. Thus the final position estimation done by fingerprinting was expressed in WGS84 coordinate system in order to be compared with results from GPS receiver.

The performance of localization service was evaluated by different criteria. These criteria are used because of more general validation of the results. The obtained results are compared by statistical characteristics – median, histogram and CEP. The CEP is defined as the radius of circle that has its centre at the final estimated location and contains the location estimated with probability P_{CEP}.

The applicable positioning accuracy results from particular location based applications. Our results are compared to FCC emergency standard [17]. The standard defines location accuracy and reliability for E-911 calls. Our system is focused on standard for handset-based solution, which requires

- 67 % of all fixes must be less than 50 m from ground truth,
- 95 % of all fixes must be less than 150 m from ground truth.

Therefore, we focused on CEP under probabilities of 67 % and 95 % (marked CEP67 and CEP95).

5 Experimental Results

In the following part we discuss results obtained in three different scenarios by means of localization service described above. The obtained positioning results for all scenarios are shown in Table 1.

Table 1. Localization error vs. scenario

Scenario	*1*	*2*	*3*	*Overall*
Median [m]	16	24	40	27
CEP67 [m]	23	37	49	36
CEP95 [m]	53	68	72	64

According to results shown in Table 1, it can be concluded, that the environment plays very important role in positioning process. The most accurate results were obtained in scenario 1. The median value is 16 meters. The localization error increases with growing number of reflectors. In case of the second scenario the median of error is 24 m. The most inaccurate results were reached in scenario 3, where a lot of movable and static reflectors could be found. The CEP67 and CEP95 values are important for implementation for emergency use. On the basis of the results, it can be claimed that the solution fulfils FCC recommendation for positioning accuracy. Overall results for all scenarios are 36 m for CEP67 and 64 meters for CEP95. These results are obviously under the thresholds (50 and 150 meters).

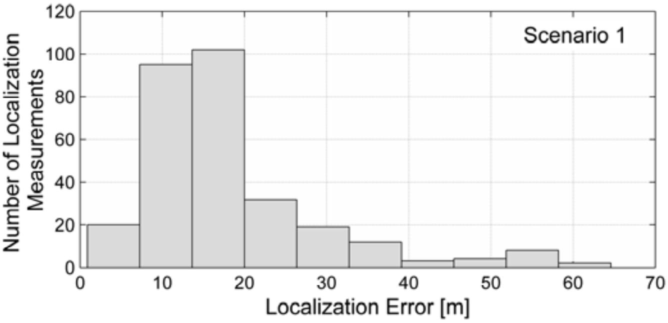


Fig. 4. Histogram of localization error for Scenario 1

Fig. 4 depicts the histogram of localization error for the first scenario. Environment in this scenario is characterized by open area with a very small number of reflectors. Line-of-Sight (LoS) signal propagation is dominant in this scenario. As can be seen in the figure, the majority of localization errors lies between 10 and 20 meters. These are very precise positioning results for GSM cellular networks. On the other hand, we have to note that these are almost ideal conditions. The localization error histogram for the second scenario is shown in Fig. 5.

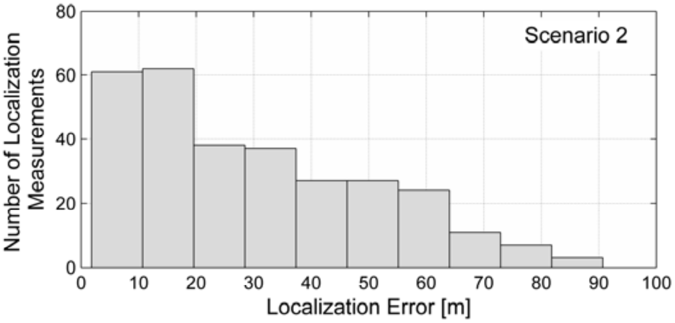


Fig. 5. Histogram of localization error for Scenario 2

According to Fig. 5, there is greater localization error in scenario 2 than in scenario 1. The reason is the different environment, which is characterized as open area with many movable reflectors. The positions of these reflectors are different between offline phase and online phase. We suppose that this fact causes accuracy decrease and increase of number of higher localization errors.

Fig. 6 shows the histogram of localization error for the third scenario. The environment can be described as urban area with many buildings and movable reflectors. NLoS and multipath signal propagation is dominant in this scenario. As shown in Fig. 6 the localization error is more distributed compared to previous scenarios and it is the highest. This is caused by hostile environment. There is significant difference between data from database (radio map) and data measured during positioning.

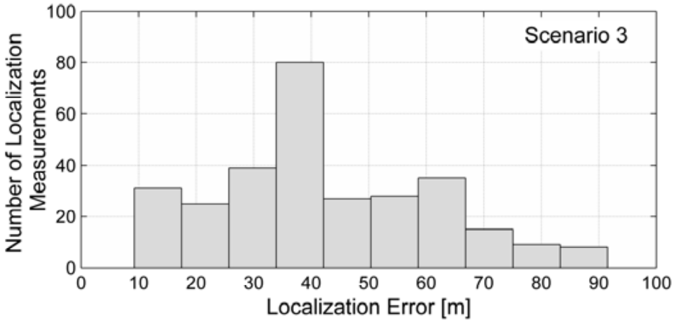


Fig. 6. Histogram of localization error for Scenario 3

Table 2 compares implemented fingerprinting solution with other localization methods in GSM network. It is obvious that fingerprinting provides generally better results than other methods except AGPS used in GSM network. An implementation costs for this method are small, because it is not necessary to modify mobile terminals and radio map could be created by means of sophisticated simulation tool. The positioning results could be also sufficient under precise environment map condition.

Table 2. Comparison of localization methods [18]

Name	*Localization Error*
Cell Identity	100 m – 39 km
Cell Identity + Timing Advance	555 m
Received Signal Strength	100 m – 3 km
RSS + AGA [7]	100 m – 700 m
Enhanced Observed Time Difference	50 – 200 m
Time Difference of Arrival	100 – 200 m
Angle of Arrival	150 m
Fingerprinting	53 – 72 m
Assisted GPS (AGPS)	5 – 30 m

6 Conclusion and Future Works

We proposed and verified positioning solution based on fingerprinting method and GSM. The solution utilizes received signal level information. The proposal is implemented as mobile-assisted positioning. The MS collects the necessary data from surrounding base stations. The measured data are sent from mobile terminal to the localization server for position estimation. The server estimates position and the information about position is sent back to the terminal. Position information is displayed in the map on terminal screen. There is no significant performance at mobile station required to localize itself, because this is handled by servers, which are components of the network.

The experiments were realized in three significantly different scenarios from propagation condition point of view. We can observe hostile shadowing, multipath propagation and almost ideal radio channel on the other hand. Therefore, we can conclude that the performance of the location based service was validated in the representative samples of environment. The obtained results fulfil FCC recommendation for positioning accuracy in emergency calls, i.e. CEP67 is 36 m and CEP95 is 64 meters.

Fingerprinting accuracy can not compete with GPS technology but it can help if GPS signals are too weak. There are various ways for further research and improvements. At first, localization could be improved by using more advanced algorithms such as KNN, SMP, neural networks or Bayesian modeling. Also execution of multiple measurements at one spot and Kalman filtering of input data could have positive impact on positioning accuracy. Secondly, the process of radio map creation could be either replaced by radio coverage model or at least some data could be extrapolated.

At last, system could be extended for indoor localization, however with some necessary modifications in the process of radio map creation.

Acknowledgments

This work has been partially supported by the Slovak VEGA grant agency, Project No. 1/0392/10 “The research of mobile nodes positioning in wireless sensor networks”, the Slovak Research and Development Agency under the contract No. LPP-0126-09 and by

Centre of Excellence for Systems and Services of Intelligent Transport
ITMS 26220120028
Project co-financed by the European Union
European Regional Development Found

References

1. Location Based Services Forecast from ABI Research, http://www.twine.com/item/11djpjdj2-172/location-based-services-forecast-from-abi-reserach
2. GSM Association, Market Data Summary (Q2 2009) Connections by Bearer Technology (2009), http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm
3. Wang, X., Wang, Z., O’Dea, B.: A TOA-based location algorithm reducing the errors due to non-line-of-sight (NLOS) propagation. IEEE Transactions on Vehicular Technology 52(1), 112–116 (2003)
4. Deligiannis, N., Kotsopoulos, S.: Mobile Positioning Based on Existing Signalling Messaging in GSM Networks. In: Proceedings of 3rd International Mobile Multimedia Communications Conference (MSAN), Nafpaktos (2007)
5. Brida, P., Cepel, P., Duha, J.: Mobile Positioning in Next Generation Networks (Chapter XI). In: Kotsopoulos, S., Ioannou, K. (eds.) Handbook of Research on Heterogeneous Next Generation Networking: Innovations and Platforms, pp. 223–252. IGI Global, New York (2008), ISBN 978-1-60566-108-7
6. Krejcar, O.: User Localization for Intelligent Crisis Management. In: 3rd IFIP Conference on Artificial Intelligence Applications and Innovation (AIAI 2006), Athens, Greece, June 07-09, vol. 204, pp. 221–227 (2006), ISSN: 1571-5736
7. Brida, P., Cepel, P., Duha, J.: A Novel Adaptive Algorithm for RSS Positioning in GSM Networks. In: CSNDSP 2006 Proceedings, Patras, pp. 748–751 (2006), ISBN 960-89282-0-6
8. Anne, K.R., Kyamakya, K., Erbas, F., Takenga, C., Chedjou, J.C.: GSM RSSI-based Positioning Using Extended Kalman Filter for Training ANN. In: IEEE Vehicular Technology Conference, Los Angeles, vol. 7(60), pp. 4141–4145 (2004), ISBN: 0-7803-8521-7
9. Laitinen, H., Nordstrom, T., Lahteenmaki, J.: Location of GSM Terminals Using a Database of Signal Strength Measurements. In: URSI XXV, National Convention on Radio Science, Helsinki (2000)
10. Takenga, C., Kyamakya, K., Quan, W.: On the Accuracy Improvement Issues in GSM Location Fingerprinting. In: Vehicular Technology Conference, VTC-2006 Fall, Hannover, pp. 1–5 (2006), ISBN 1-4244-0062-7

11. Nerguizian, C., Despins, C., Affes, S.: Indoor Geolocation with Received Signal Strength Fingerprinting Technique and Neural Networks. In: de Souza, J.N., Dini, P., Lorenz, P. (eds.) ICT 2004. LNCS, vol. 3124, pp. 866–875. Springer, Heidelberg (2004)
12. Hata, M., Nagatsu, T.: Mobile Location Using Signal Strength Measurements in a Cellular System. IEEE Trans. on Vehicular Technology VT-29, 245–252 (1980)
13. Wong, C.L.C., Lee, M.C., Chan, R.K.W.: GSM-based mobile positioning using WAP. In: Wireless Communications and Networking Conference (WCNC), vol. 2, pp. 874–878 (2000)
14. Otsason, V.: Accurate Indoor Localization Using Wide GSM Fingerprinting, Master's thesis, Tartu (2005)
15. Kurner, T., Meier, A.: Prediction of outdoor and outdoor-to-indoor coverage in urban areas at 1.8 GHz. IEEE on Selected Areas in Communications 20 (2002)
16. Kolodziej, K.W., Hjelm, J.: Local Positioning Systems, LBS Applications and Services, pp. 156–157. CRC Press, Boca Raton (2006), ISBN 978-0-8493-3349-1
17. WTB/Policy: FCC Wireless 911 Requirements (2001)
18. Brida, P.: Location Technologies for GSM. In: Proceedings of 5th European Conference of Young Research and Science Workers in Transport and Telecommunication TRANSCOM, Zilina, pp. 119–122 (2003), ISBN 80-8070-081-8

Customized Contents Service Over a DVB-SH/3G Network

Azza Jedidi and Frédéric Weis

INRIA,
IRISA, Campus de Beaulieu, France
`{azza.jedidi,frederic.weis}@irisa.fr`

Abstract. Next generation networks aim at delivering more and more sophisticated rich multimedia applications. Such applications are supposed to be personalized, interactive and available at high data rates. Recent researches generally propose the convergence and cooperation between different networks, in order to fit future application needs. In this context, we first worked on the coupling between a DVB-SH network, which is a high capacity unidirectional broadcast network and a 3G cellular network, which provides interactivity. We highlight the possibilities offered by such a cooperation through the definition of different scenarios of mobile TV services. Then, we considered the coupling between DVB-SH and MBMS networks. MBMS is an evolution of UMTS cellular network, which brings multicast and broadcast capacities, with a fine grained localization of services. In this paper we focus on enriching classical DVB TV services with customized contents delivered via 3G-MBMS path, in order to target very localized user communities[1].

Keywords: Next Generation Networks, convergence, DVB, 3G, MBMS, multimedia, personalized and localized services, mobile advertising.

1 Introduction

Recently, a growing interest has been shown in multimedia networking mainly due to the emergence of efficient audio/video encoding techniques and the proliferation of enhanced audio-visual services. The demand for these kinds of applications has quickly increased. Major advances in communication and network technologies have made multimedia services technically and economically doable in any type of environment. Digital TV and multicast IP represent the best processes to deliver multimedia content respectively through broadcast and Internet-based networks. Regarding broadcasting standards, Digital Video Broadcasting

---

[1] This work has been done within the TVMSL (*TéléVision Mobile Sans Limite*) project led by Alcatel-Lucent. This project plans to develop a DVB-SH standard suitable for hybrid satellite and terrestrial transmission. It is supported by the French innovation Agency OSEO.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 710–721, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

(DVB) is expected to be the prominent European television broadcast standard for the next decades, as well through a satellite-based technology (DVB-S) , as in terrestrial television (DVB-T), cable (DVB-C)or for hand-held devices (DVB-H). The DVB technology provides relatively high bandwidth data channels but based on uni-directionality, thus neglecting interactivity. DVB-SH, satellite services for hand-held devices, is a hybrid (satellite / terrestrial) architecture. It is defined as a system for IP based media content and data delivery for hand-held terminals, via satellite. Satellite transmission guarantees wide area coverage. Moreover, it is coupled with terrestrial gap fillers assuring service continuity in areas where the satellite signal cannot be received (built-up areas for example). DVB-SH provides users with a variety of services, which could be classified in several categories. It offers real-time applications. Examples are TV-like broadcasting, live broadcasting and notification, which consists in broadcast notifications sent according to the preferences of the user (notifying a football fan of the retransmission of his preferred team matches for instance) and games, like real-time quizzes or multi-player online role-playing games, etc. It also provides applications to download. For large general audiences, data file purchase services are offered, either on a subscription basis, such as downloading every morning the electronic version of the user's newspaper, or on an impulsive purchase basis, like for films, books and audio CD purchase. Besides, one of the main characteristics of the Internet world is its bidirectionality, permitting full interactivity to users. In this project, a DVB-SH broadcast network is combined with a 3G cellular network to ensure this bidirectionality. Actually, this convergence takes benefit from 3G and DVB networks. 3G network characteristics, especially upload link, enable added-value services and applications that are interactive and more personalized. DVB-SH is provided with a very high bandwidth capacity that allows unidirectional IP-TV channels broadcast. In our previous studies, we defined several scenarios of services where we switched 3G popular services over the DVB path [1,2].

In this paper, we propose a new scenario of service. We consider classical DVB channels, including TV programs and advertisements spots. We enhance such a TV service through the definition of personalized advertisements spots, that better fit user interests and localization. Obviously, advertisements are here given as an example of personalized service, but other types of contents can be proposed. In this scenario, the personalized content is sent over 3G, while the DVB content is still broadcasted. The terminal entity receives both contents, but plays only the personalized one. An important issue here will be the synchronization of flows to be read. The paper is organized as follows. The next section presents related work to DVB/3G inter-working. Section 3 describes the system architecture and the service scenario. The necessary signalization mechanisms are detailed in section 3.3. Section 4 validates our simulation of the scenario progress, and presents some observations and results. Section 5 proposes an enhancement of the scenario through the use of MBMS network, and its multicast broadcast capacities. Finally, section 6 draws our conclusion.

2 Related Work

Mobile advertising is a major applications of next generation networks. Advertisements could be customized based on user's location or on his main interests or on the TV programs he is watching.

Localized advertising covers the insertion of locally relevant advertisements. The goal is to provide users with advertisements concerning facilities in the nearer surrounding of their location [3], [4], [5]. In the currently deployed localized advertisement architectures, advertisements are generally ingested into a network accessible library and identified with a unique metadata. Standardized interfaces exist between this library of advertisements, the splicer, which is the equipment responsible of placing the advertisment in the video stream, and the scheduling server. At the appropriate time, the splicer inserts the local advertisement into the national feed [6].

Personalized advertisements can target the demographics associated with a household, a set-top or even an individual user. Search engines target advertisements based on search criteria a user enters. Retail web sites have long made suggestions for new products and services based on a user's previous order history, or on what others who have made similar purchases were also interested in, or on logical merchandising assumptions that suggest ancillary products.

Content based advertising are advertisements that target viewers based on their viewing patterns by advertising during certain programs or on certain networks. In this work, we take benefit of the coupling between DVB and 3G path to provide personalized TV contents, through 3G unicast. At first, we propose personalized advertisements based on user profiles, provided during the subscription process. Then, we propose localized advertisements thanks to a DVB-MBMS coupled networks.

3 Personalized Content Delivery Over a DVB-SH /3G Network

We consider a DVB TV channel proposed to users in two versions.

1. The Basic service: This is the "classical" DVB channel. The content is made of TV programs and advertisements which are broadcasted to all subscribers. In this service, the same advertisement spot is received by all users.
2. The Premium service: In this version of the service, the same TV programs are still broadcasted to users. However, during the advertisements, users receive advertisements sequences that correspond to their main interests. In this scenario, a user provides a profile that indicates his main interests when subscribing.

3.1 Architecture

In this scenario, we have chosen to consider personalized advertisements. Obviously, other customized services and contents could be proposed. The personalized contents are stored in 3G content servers. DVB-SH TV channel delivers Electronic Service Guide (ESG) messages announcing its programs and services. A mobile user receives the ESG messages and decides to subscribe to the TV channel. He can choose either the Basic or the Premium service. In this scenario, the user chooses to subscribe to the Premium version of the service. As a consequence, a subscription request and a user profile are delivered to the subscription module, through 3G uplink. The user profile indicates user's main interests.

In our approach, users have actually to choose from a list of possible interests. Their choice is transmitted to the subscription module, which is located in a Unicast Broadcast Router (UBR), as shown in figure 1. This router is the central equipment of our DVB-3G converged network. We designed this equipment to manage the DVB-3G network services (subscription, flow scheduling, signalization, synchronization, etc.). The UBR corresponds to the Service Management entity in DVB IP DataCast standard [8]. In our scenario the UBR contains the list of Premium service users and their interests. After subscription, the user starts receiving the broadcasted DVB channel. In this step, all subscribers (Basic ones and Premium ones) receive the same TV program, over the DVB path. On 3G side, there are several content servers, providing different content thematics.

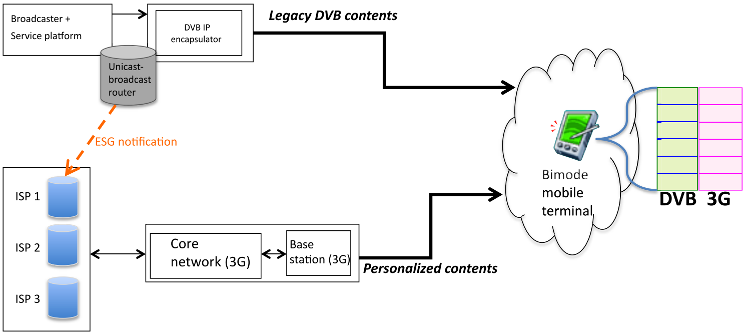


Fig. 1. Coupling DVB with 3G network

3.2 Scenario Processing

Before advertisement start, DVB server sends a notification message to each of its 3G personalized content servers. We use an ESG message for this notification, this point is discussed in section 3.3. This signalization message notifies of the scheduled time of the next advertisement. At advertisement time, the DVB TV program is interrupted and the DVB advertisement spot starts. Basic service mobile users receive and play this spot, in their terminal. Premium service mobile users continue receiving the DVB flow on their terminal. Actually, the reception of the DVB channel is not interrupted during the advertisement. At the same time, they receive and play a personalized advertisement through 3G unicast. The terminal receives both advertisements (the DVB one and the 3G one) but only plays the personalized 3G one. In this scenario, we assume that user terminal is bimode and manages two memory areas one for DVB flows and the other for 3G flows, as presented in figure 1. At advertisement start, the terminal player switches from the DVB memory area to the 3G one, so that it plays the personalized content. At advertisement end, the terminal returns back to playing its DVB memory area content.

Main problems. In this scenario, we have to treat several challenging issues. First, at least a part of the customized 3G advertisement should be available on terminal 3G memory area and ready to be played right on time. Then, the terminal player should possess an accurate and precise synchronization information in order to operate a smooth and seamless switching. Moreover, we had to define the appropriate signalization messages to ensure the communication between the different involved equipment and last but not least we had to consider the network scalability problems when the number of Premium users increases.

3.3 Definition of ESG Signalization

Service announcement message. DVB users receive all messages broadcasted over DVB, including ESG messages that announce the coming programs and services. Those are classical ESG XML messages [9], delivered over DVB-SH. In our scenario, they announce the coming programs. They also announce the possibility to subscribe either to the Basic version of the service or to the Premium version, with personalized content. Subscription requests are sent to the subscription module over 3G uplink. During the subscription process, Premium users are asked to deliver a user profile that indicates their main interests, in order to receive advertisements that best fit their expectations.

Advertisement transmission time message. After subscription, the service starts. The DVB programs start being broadcasted. The DVB operator sends a notification message to the 3G content servers to order advertisement transmission start. This order occurs slightly before advertisement scheduled playing time, as we take into account 3G transmission delays, in order to start the advertisement playing on time. Actually, at advertisement scheduled playing time, at least a part of the personalized advertisement is already in the terminal memory, ready to be played instantaneously. For this notification, we chose to use an ESG message. Actually, we studied the ESG XML structure and deduced that it provides the necessary fields for our message. An ESG message is structured as XML fragments [9], as shown in Figure 2. The Schedule Event Fragment is compound of several fields. In particular, the *ContentFragmentRef* field is used to reference a Content fragment, which describes the content available during this Schedule event. The schedule event fragment is the appropriate ESG fragment to be used to schedule our advertisement transmission start event.

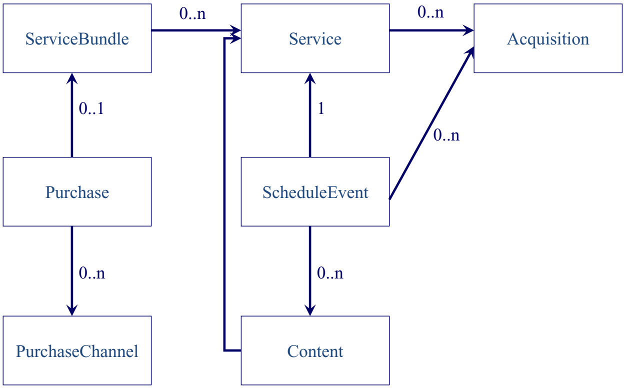


Fig. 2. ESG XML fragments

Synchronization information message. DVB operator also sends a signalization message to the mobile terminals. This message gives Premium service terminals the necessary information in order to play their flows and seamlessly switch between DVB content and 3G customized content playing, without service interruption. For this ESG message, the schedule event fragment could also be used to give the synchronization information and schedule the play switching event.

The terminals play their DVB program (that is received on their DVB memory area). Then, during the advertisement time, they continue to receive the DVB flow. However, they do not play it. They switch to their 3G memory area, where they have already received at least a part of the personalized advertisement (and the rest is being received). The 3G advertisement is played. At advertisement scheduled end time, terminals switch back playing the DVB content.

It is important here to operate a very smooth and precise switching, in order to make Premium users restart playing the DVB program at exactly the same moment as the Basic service users. Actually, it could be very disturbing to switch back to DVB playing when DVB advertisements are still being played, or when the DVB programs have restarted a while before.

We propose to use a marker in the DVB flow itself, that will design the exact frame where the switching has to occur. Our approach lead us to propose either the MPEG-2 TS Sync byte, which is a marker dedicated to synchronization or to give the number of the burst corresponding to the switching moment. In this context, we still have not a definitive choice and it is possible to investigate different fields that could provide the most accurate synchronization information.

4 Validation of the Scenario

For our simulations, we evaluated several tools, and we finally chose to use OPNET Academic edition simulator [7] since it is more adapted for realistic large-scale scenarios. Using OPNET, we have simulated the functional entities of our architecture. Indeed, the implementation of many components was needed, for example DVB content creation, ISP application server, UBR router, DVB/3G networks and mobile terminals.

4.1 Simulation and Results

On DVB side, a TV channel is broadcasted at 384 Kbits/s data rate.

On 3G side, there are several content servers where the personalized content are stored. Those servers receive the order from the DVB operator, to send the advertisements at the right time. The 3G contents are delivered at a 256 Kbits/s data rate. We chose this value as it represents the classical throughput offered to a 3G mobile user.

At simulation start, users receive the broadcasted ESG messages. They can subscribe to the DVB channel. They choose either the Basic service or the Premium one. Subscription requests are sent to the subscription module over 3G uplink. During the subscription process, Premium users provide a user profile that indicates their main interests, in order to receive advertisements that best fit their expectations. After subscription, the service starts. And the DVB program is broadcasted. The DVB operator sends a notification message to the 3G content servers to schedule advertisement transmission. Another ESG message is sent to the terminals. This synchronization message is presented in paragraph 3.3. At advertisement start, the DVB program is interrupted, and a DVB advertisement sequence is broadcasted to all users. The Basic service users receive and play the DVB advertisement. The Premium service users continue receiving the DVB flow. However, as they subscribed to the Premium service, they receive personalized advertisements through 3G. Thus, they use the synchronization information they had received, in order to switch to the personalized advertisement playing and then switch back to the DVB flow when the advertisement ends. Obviously, we consider advertisements with the same durations, for synchronization reasons. Figure 3 shows the flows received by a Premium service user terminal, respectively on DVB and on 3G dedicated memory areas. Effectively, DVB flow

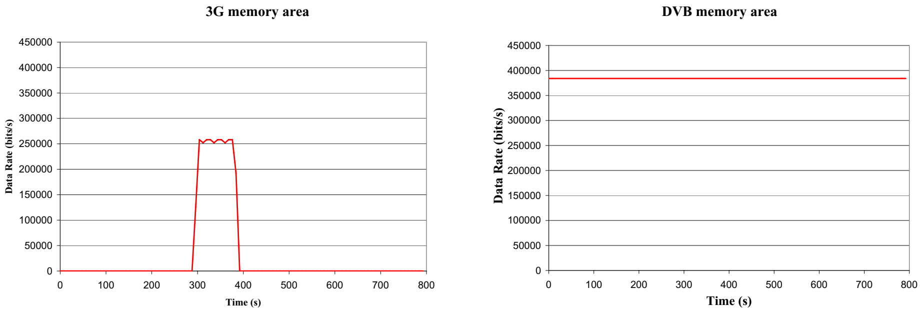


Fig. 3. Terminal received flows

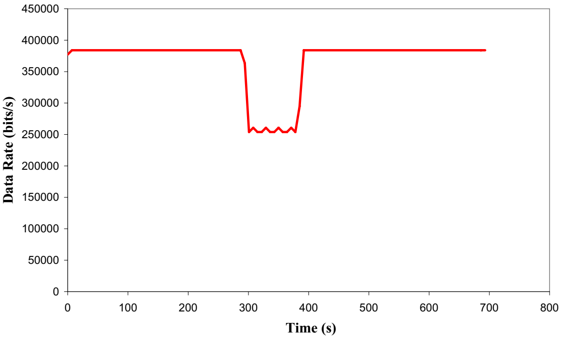


Fig. 4. Terminal player

reception does not stop during the advertisement sequence. The terminal receives simultaneously the DVB and the 3G advertisements. Actually, during the advertisement sequence, both DVB and 3G contents are received. However, during the advertisement time, the Premium user terminal plays only the 3G personalized advertisement. Figure 4 shows the flows played on the terminal player. Effectively, the terminal player operates a smooth and precise switching from DVB TV program playing to 3G personalized advertisment playing, thanks to the provided ESG synchronization information. Then, the terminal returns back playing the DVB TV program at the advertisment end.

4.2 Analysis of the Results

Implementing our scenario on OPNET simulation tool and running several simulations have permitted the functional validation of our scenario of service.

In this scenario, we proposed an interesting enhancement of our mobile TV service. In fact, in addition to the Basic version of the DVB mobile TV service with a general content adressed to all users and broadcasted over DVB path, we propose a Premium version of the service, available on a subscription basis. The TV programs are still provided over DVB, while, other customized contents are provided through 3G unicast. For instance, those contents could be advertisements. They are chosen based on the user profile, and sent in a 3G unicast mode.

An important criteria of scenario performance is the scalability of the service. So we progressively increased the percentage of Premium service users while evaluating the impact on 3G network performances. Of course, the deployment of customized advertisement service will lead to many 3G unicast connections. This deployment could prejudice 3G network performances. Actually, the 3G network provides our personalized advertisements in addition to its own services (FTP, HTTP, Mail, Voice, etc.). The delivery of personalized advertisement over the 3G path is not supposed to degrade the 3G network "legacy" services performances. The problem is that a 3G base station has a limited power. The maximum value of a Node B power transmission is generally of about 20 watts [10] [11].

Deploying more and more unicast connections to serve the customized contents leads to an over exploitation of 3G base station and can disturb the performances of 3G classical services, leading to congestions and even service disruption. So the current scenario is not scalable as is and necessitates several enhancements.

Looking further to our scenario principle led us to an important observation: In many cases, a group of users sharing the same location, have often similar interests. For example users can attend the same event (a concert), and so they are potentially interested in receiving information related with this event. As a consequence, it seems interesting to provide users with customized contents based on their location, rather than providing them with personalized contents based on their user profiles. Users sharing the same location will now receive the same content, thus reducing the number of deployed connections.

Starting from this observation, we decided to adapt our architecture to the new scenario need's. In the remainder of this paper, we couple our DVB-SH network with an MBMS network (Multimedia Broadcast Multicast Service). MBMS is an evolution of UMTS (UMTS release 6) [12]. Its offers an evolved 3G multicast broadcast solution over a 3G cellular network. The most important issue about MBMS is that it offers a fine grained localization capacity. This last property is very valuable in the context of our localized advertisement service as it will allow the delivery of one specific content per radio cell.

Premium service users, sharing the same location (i.e. same radio cell), are going to receive the same content. This content is tightly coupled to users location. This could be advertisment for the local hotels, restaurants and shops, or some tourism information or even advertisements for local music or sport event.

5 Localized Content Delivery Over a DVB-SH /MBMS Network

For the rest of our study, we coupled DVB-SH with a 3G-MBMS network, and we try to provide a different localized advertisement in each radio cell. Thanks to MBMS, we no more have to deploy many unicast connections to serve our users. We simply define multicast groups based on users' location. The advantage of MBMS is that it allows many receivers in the same radio cell to be served by a common signal transmission facility, or bearer, thus conserving radio resources (cf. figure 5).

5.1 Presentation of a MBMS Network

MBMS Multicast and Broadcast mechanisms. The main attraction of MBMS is that it allows many receivers in the same radio cell to be served by a common signal transmission facility, or bearer, thus conserving radio resources. This is not a new idea in UMTS.

MBMS uses IP multicast packets, that is, packets sent to a class D IP address, but the GGSN and SGSN send multicast packets only once to each downstream node. More importantly, packets are transmitted only once in each cell, at least

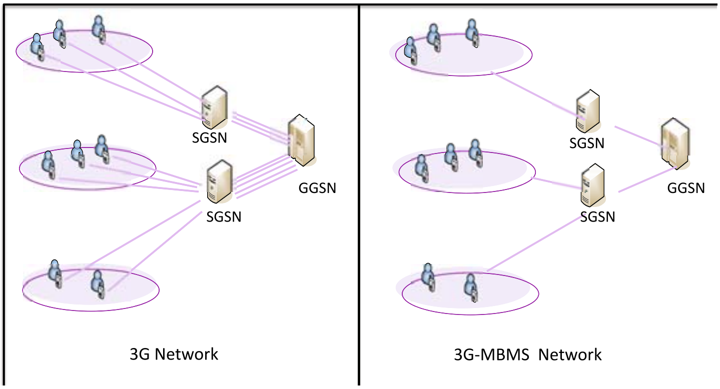


Fig. 5. IP multicast with MBMS

when a sufficient number of intended receivers is present there. In fact, while MBMS can potentially provide considerable savings in transmission bandwidth over the air, it incurs considerable signaling overhead and may not even make sense for small numbers of users.

MBMS architecture. The Broadcast/Multicast Service Center (BM-SC)is the new functional entity added to the packet switching domain of the UMTS core network. It plays a mediating role between the content providers and the UMTS network, as shown in Figure 6. The BM-SC is responsible for both the control and user planes of an MBMS service. It is also responsible for authenticating and authorizing the content providers, receiving and possibly modifying their data. For instance, it encryptes and passes these data to the GGSN for transmission. The BMSC may repeat a whole data transmission or specific parts of it for error recovery purposes. It also brings information about its services for service announcement and bearer setup purposes. Moreover, it screens the UEs wishing to join a multicast session to verify whether they have subscribed to the service. Then, it initiates the session start and stop phases.

MBMS, not only adds a new node to the UMTS architecture, but also requires modifications to existing nodes.

The Gateway GPRS Support Node (GGSN) is responsible for transmitting data via tunnels to the appropriate Serving GPRS Support Nodes (SGSN), that is, all SGSNs in the case of broadcast services or only those SGSNs serving group members for multicast services. The SGSN sends these data via tunnels to the appropriate RNCs or BSCs, depending on whether the UTRAN or the GERAN is used. During the session start phase, the SGSN instructs the RAN to establish actual radio bearers. Then, during the session stop phase, it instructs the RAN to release the actual radio bearers [12]. Finally, the User Equipment (UE) is responsible for joining and leaving multicast services and for enabling or disabling broadcast services. It also has additional application specific tasks, like media playback for example.

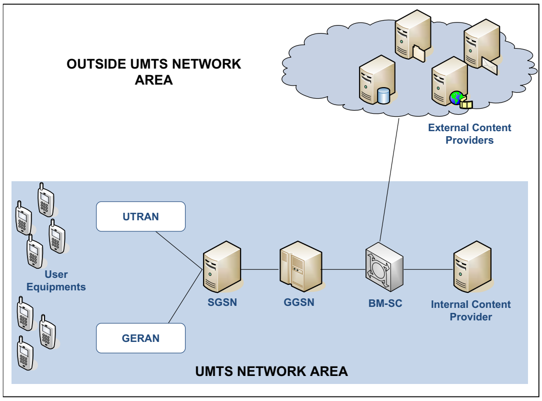

OUTSIDE UMTS NETWORK AREA
External Content Providers
UTRAN
User Equipments
SGSN
GGSN
BM-SC
Internal Content Provider
GERAN
UMTS NETWORK AREA

Fig. 6. MBMS architecture

5.2 Simulation and Main Results

OPNET simulation tool provides an implementation of UMTS, but does not implement MBMS network. For our simulations, we used an OPNET implementation of MBMS network, which was developed in the framework of B-BONE European project [16]. For this new simulation, we maintain the simulation parameters used in section 4.

Let us focus on one MBMS radio cell. Mobile users are moving in the cell at varying speeds. Terminals are bimode. They receive the DVB TV programs. They also receive 3G legacy services (email, FTP, HTTP, etc.). Some of them may be Premium users of our TV service. Those ones will receive the localized video at advertisment scheduled time. In our simulations, we increase the number of Premium service users and study the impact of MBMS network use on our scenario performances. As expected, MBMS deploys only one multicast connection per radio cell, to deliver the local advertisment. Thus, each Premium user benefits of an advertisment adapted to his location, and 3G network performances are preserved as we no more deploy numerous unicast connections for our service.

6 Conclusion

In this paper, we specified the basis for the deployment of customized services over DVB-SH / 3G coupled network. The main idea was to punctually replace DVB-SH legacy programs by 3G contents, that better fit users' needs and interests. This substitution is managed by the terminal, and the synchronization is processed using specific ESG messages. The problem with such a service is its scalability, considering the risks of saturating 3G network with the unicast delivery of personalized contents. As a solution to this problem, we proposed to use MBMS services, that provide multicast/broadcast mechanism on a 3G network. Thanks to MBMS, we replace the personalized advertisements delivered via 3G unicast by localized contents offered via multicast, thus preserving the performances of 3G network legacy services.

References

1. Jedidi, A., Tlais, M., Weis, F.: Coupling 3G with DVB Networks for Low Cost Services. In: 3rd International Conference on Engineering Management and Service Sciences, Special Session on Media Interactivity and Network Convergence, Beijing, China (September 2009)
2. Jedidi, A., Tlais, M., Weis, F., Kerboeuf, S.: Efficient Switched Services over a DVB-SH/3G Network. In: 5th International Mobile Multimedia Communications Conference, London, UK (September 2009)
3. Aalto, L., Göthlin, N., Korhonenm, J., Ojala: Bluetooth and WAP Push based location aware mobile advertising system. In: MobiSYS 2004 Proceedings of the 2nd international conference on Mobile systems, applications and services, Boston, USA (2004)
4. Kolmel, B., Alexakis, S.: Location based advertising. In: Proceedings of the 1st international conference on mobile business, Athens, Greece (2002)
5. Ververidis, C., Polyzos, G.: Mobile marketing using a location based service. In: Proceedings of the 1st international conference on mobile business, Athens, Greece (2002)
6. UDCAST: DVB-H mobile tv flexible satellite distribution, European Standard ETR 154 (January 2007)
7. `http://www.opnet.com`
8. EBU/ETSI: Digital Video Broadcasting (DVB) IP datacast over DVB-H: Architecture, European Standard ETSI TR 102 469
9. DVB IP DataCast over DVB-H Electronic Service Guide (ESG), DVB Document A099 Rev.1 (September 2008)
10. Alexiou, A., Bouras, C., Kokkinos, V.: Evaluation of different powersaving techniques for MBMS services (October 2008)
11. `http://www.sante.gouv.fr/htm/actu/telephonemobile070201/dplieux.htm`
12. Xylomenos, G., Vogkas, V., Thanos, G.: The Multimedia Broadcast/Multicast Service. Wireless communications and mobile computing 8(2), 255–265 (2008), ISSN 1530-8669
13. Annamalai, M.: Multimedia Broadcast Multicast Service (MBMS) in GSM based wireless networks, T-mobile USA, Technical report (April 2004)
14. 3GPP: Multimedia Broadcast/Multicast Service (MBMS) user services; Stage 1, V6.2.0 (2004)
15. 3GPP: Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs, V6.2.0 (2005)
16. MBMS System Level Simulator, `http://b-bone.ptinovacao.pt/`

Measurement and Visualization of ECG on Mobile Monitoring Stations of Biotelemetric User Adaptive System

Dalibor Janckulik, Leona Motalova, and Ondrej Krejcar

VSB Technical University of Ostrava, Center for Applied Cybernetics,
Department of Measurement and Control, Faculty of Electrical Engineering
and Computer Science, 17. Listopadu 15, 70833 Ostrava Poruba, Czech Republic
Dalibor.Janckulik@hotmail.com, Leona.Motalova@gmail.com,
Ondrej.Krejcar@remoteworld.net

Abstract. Adaptivity and friendliness of user interface is currently discussed in the professional society. Users want a simple, intuitive and graphically attractive interface. On the other hand, it is necessary to change dynamically the user´s experience as they use what best viewing area of the device. The biomedical data are not all the latest knowledge in the area. Our work focuses on exploring the possibilities and the revelation of any deficiencies in the currently used procedures and technologies. The main area of interest of our Biotelemetric User Adaptive System is to provide solution which can be used in different areas of health care and which will be available through PDAs (Personal Digital Assistants), web browsers or desktop clients. In paper we deals with a problem of visualization of measured ECG signal on mobile devices in Real Time as well as with a solution how to solve a problem of unsuccessful data processing on desktop or server. The pre-processing in GSM module processor we choose as a solution of data processing problem.

Keywords: User Adaptivity, Real Time**,** PDA, Embedded Device, Biotelemetry, ECG, Silverlight, WPF, Dynamical Programming, XML.

1 Introduction

The basic idea is to create a system that controls important information about the state of a wheelchair-bound person (monitoring of ECG and pulse in early phases, then other optional values like temperature or oxidation of blood etc.), his situation in time and place (GPS) and an axis tilt of his body or wheelchair (2axis accelerometer). Values are measured with the existing equipment, which communicates with the module for processing via Bluetooth wireless communication technology. Most of the data is processed directly in PDA or Embedded equipment to a form that is acceptable for simple visualization. The next problem is about data processing is ECG packets parsing which can’t be processed with real-time response on PDA or embedded device. This restriction can be solved trough the solutions proposed as software in (Section 3) also as hardware solution in (Section 4). The sample architecture of the developed system is sketched on (Fig. 1).

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 722–738, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

User adaptivity of the system is an important part of different platforms to work with biomedical data. GUI should be realigned according to various parameters and sensed perceptions so that what at first glance most of describing the situation. Our system reacted too to stimuli from the hardware used by devices such as light sensors, accelerometers, GPS and GSM module. The main aim of the platform for patients' bio-parameters monitoring is to offer a solution providing services to help and make full health care more efficient. Physicians and other medical staff will not be forced to make difficult and manual work including unending paperwork, but they will be able to focus on the patients and their problems. All data will be accessible almost anytime anywhere through special applications designated for portable devices web browser or desktop clients and any changes will be made immediately at disposal to medical staff based on the security clearance.

For the physicians is important see the data directly and clearly on the maximum possible viewing area. This problem can be solved by dynamical programming, when we can load only important controls and functional code from database and via dynamicaly controls hiding in GUI on presentation layer. All this possibilities are described in the following sections.

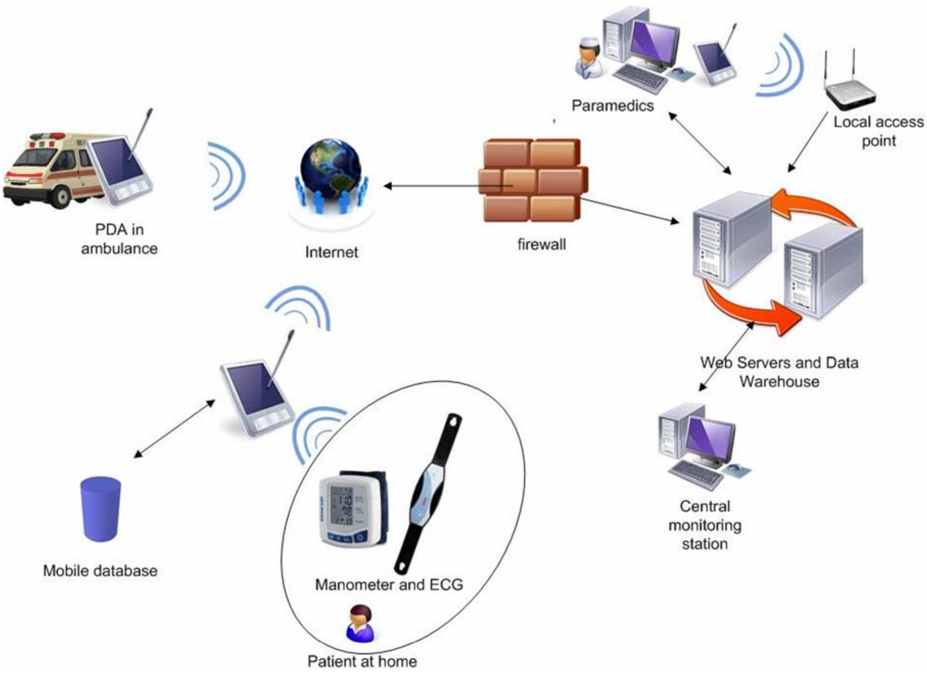


Fig. 1. Sample architecture of one option of system implementation

From the database perspective and bio-signals analysis are the data are stored and automatically analyzed by simply neuronal network.

2 The User Adaptivity of the System

The user adaptivity of the system can be divided into several areas:

- Interaction with the user is based on:
    - used equipment
    - application usage
    - used environment
- Interaction with hardware devices based on the usage of applications

2.1 Adapting Based on the Used Equipment

The application responds as the most of applications on the resolution imaging devices - displays – on the placement of elements. For client applications, where user fills in or views his personal records, the application will behave in different ways while running on personal computer or running on mobile devices such as PDAs with QVGA, VGA or WVGA resolution. For the mobile platform many controls are not available, but we also need to adjust the controls for equipment or touch SmartPhone with a keyboard. Features in one desktop application form must be in the mobile application divided into logical groups. Elderly people may have difficulties with fine resolution and small font, the younger generation will not mind that and we can put in more information into the form.

2.2 Adapting Based on the Usage of Applications in Terms of Interaction with the User

A client application for an average user is responsible for, as already described above, showing data of the user. In the case of desktop, the monitor cannot be easily manipulated and rotated as we like it. In the case of the most wide-spread tablets text information can be shown in more natural form for reading (in height of the book). On the contrary, the graph is better to be displayed in width, so that the longest record gets on the screen. The same goes for using your mobile PDA. This functionality is available for devices with accelerometer, or even for devices without accelerometer, whose display can be rotated by the user's request button.

One of the novelties is a frequently used battery indicator color change. This is for the battery of mobile devices (tablets, PDA) as well as for the battery of device designed for collecting data (ECG).

Other features are associated with the popular monitoring of heart rate during exercise. The ECG, which we get we can determine the heart rate. Blue ECG device detects a pulse back. The frequencies of training rate are obtained from the users' data and each zone is indicated by color. So the user can simply by a glance get to know in which zone his heart works.

2.3 Adaptation Based on the Environment

Here the user interface adaptation takes place according to the conditions in which it is used, at night in hospitals we do not want the monitor to light and be disruptive, but it must be legible. The solution is to switch the colors GUI so that the contrast ratio of application isn't extremely disturbed. The influence is the backlight display device that makes it possible.

2.4 Interaction with Hardware

If the user views only historical records, it does not make any sense to have the Bluetooth on; data transfer is realized using WiFi or GPRS. Compression is related, or transfer of requested data. GPRS is slow, so we transfer only data that the user actually requested, for our WiFi connection bitrates primarily confined. Shutting down the unneeded hardware is today addressed for mobile devices, where device endurance is at one of the first places.

3 Developed Software Parts of Platform

Complete proposition of solution and implementation of the patient's biotelemetry platform oriented for user adaptivity requires determination and teamwork. Every single part of the architecture has to be designed for easy application and connectivity without user extra effort, but user must be able to use given solution easily and effectively. Crucial parts of the whole architecture are network servers, database servers and client applications run-able from standard desktop operating system and client applications for Windows CE based mobile devices.

3.1 Server Part

Database background of solution is built on Microsoft SQL server. One server provides only data warehouse with stored procedures, which represent data interface for other application parts. There are stored all data of medical staff and patients. Data of patients include different records such as diagnosis, treatment progress or data which are results of measuring by small portable devices designated to home care. These data represent the greatest problem, because amount of these data rapidly increase with increasing amount of patients. Due to this fact database servers are very loaded. The stored procedures (programmed by Transact-SQL language) serve basic data parsing on weak mobile devices, which have too much problems with parsing and subsequently visualization of measured data. At this time our team is focused on implementation of analytical and reporting parts for more detailed analysis of measured/collected data. Business intelligence part of SQL server is a powerful tool which allows us to create reports faster than C# application on client side.

The only possibility of running our application on all platforms is an implementation of a view and controller layer as web application. We use two different technologies. ASP.NET is purely for web application (browser independent) and for web services. The second technology is Silverlight (only for Internet Explorer and Mozilla Firefox). Silverlight application is possible to run in Out-of-Browser mode.

In order to run a web server, an operating system supporting IIS (Internet Information Services) is needed. IIS allow to users to connect to the web server by the HTTP protocol. The web service transfers data between the server and PDA/Embedded devices. Web service also read the data, sends acknowledgments, and stores the data in the database. The service is built upon ASP.NET 2.0 technology. The SOAP protocol is used for the transport of XML data.

Methods that devices communicating with the web service can use include:

- receiving measured data,
- receiving patient data,
- deleting a patient,
- patient data sending.
- RAW data parsing
- other ...

To observe measured data effectively, visualization is needed. A type of graph as used in professional solutions is an ideal solution. To achieve this in a server application, a .NET Chart Control can be used for ASP.NET 3.5. For data analysis, neural nets are a convenient solution. However, there are problems in the automatic detection of critical states. Every person has a specific ECG pattern. The Neural net has to learn to distinguish critical states of each patient separately.

3.2 Desktop Part

The desktop client application is the main and the only part of the entire platform for patients' bio-parameters monitoring, which medical staff uses directly. It is obvious, that if Guardian should optimally replace classic paperwork, simplicity and trouble-free usage of client application are very important factors, which affect whether the doctors and medical staff accept this solution with enthusiasm and solution will be fully used or not. The options of desktop client application have to be easily upgraded. Therefore it is important to reliably design architecture which will allow that. Implementation of user functions is also important. Using the platform.NET in-build characteristics and open standards such as XML, XPath and other, is crucial. Because of that it is easy to configure or upgrade application. User interface is also easy to adjust to user request or clearance. Well designed architecture allows not only easier developing to software engineer, but brings also new and useful functions to the user. The design of appropriate architecture is crucial for the next development of implemented client application, which will be easily upgraded with new functions in the future without making any expensive and demanding changes in programmatic code.

- User Interface - represents the part of application, which is made by components of user interface.
- Command Manager - associates and administrates all existing objects „Command“, which execute operations called mainly by user interface.
- UI Factories - dynamic assembling of some parts of user interface during the run of application or immediately after lunch.
- XML Navigators – reading of components of XML documents, which describe user interface.
- Configuration – reading and editing of XML files, which are designated for primary application configuration.

- Web Service Proxy - creates an impression of existence of local web services copies.
- XML - files, which are indispensable for running of entire application. These files control exact syntax, which enables their easy programmatic analysis.

XML represents great role in suggested solution. Options of this technology are used by dynamic assembling key components of graphic user interface, which enables its changing in dependence on roles or clearance of users. It is also used for easy application configuration.

3.3 Mobile Parts

The main part of the system is an Embedded or PDA device. The difference in applications for measurement units is the possibility to visualize the measured data in both Real-time Graph and Historical Trend Graph, which can be omitted on an embedded device. PDA is a much better choice for Personal Healthcare, where the patient is already healthy and needs to review his condition. Embedded devices can be designed for one user, with the option to use an external display used for settings or with the possibility of usage in extreme conditions.

The user adaptivity on mobile devices is control reorganization based on screen rotation provided by operating system. For automatical screen orientation change the mobile device must have accelerometer or G-sensor (HTC feature) implemented. The next step is color theme of application change. This feature is provided by measured level of actual lighting from built-in light-sensor. Devices which do not have this hardware parts can be set to defaults. Application reads default values from registry or from internal mobile database. Dynamically generated design for standard WindowsForm application is developed by dynamical programming technique, where small parts of application or controls source codes are inserted in database. When the application is running, the basic parts are loaded from database. Next choice for dynamically loaded design is XML generated design, described above in (section 3.2.).

Devices based on old PDA type (all devices developed before 2007 too) have a several limitations such as low CPU performance, low battery life or small display, which is possible to solve by embedded version of such mobile clients. We created a special windows mobile based embedded device. During the development process the several problems occurred. One of them and the most important was the need of a new operation system creation for our special architectural and device needs. We used the Microsoft PlatformBuilder for Windows CE 4.2 tools. The created operation system based on standard windows mobile has several drivers which we need to operate with communication devices and measurement devices.

At this time we use modern devices based on Windows Mobile 6 and newer. These devices have no limitations listed above; the only problem is higher price.

Measured data are stored on a SD Memory Card as a database of MS SQL Server 2008 Mobile Edition. The performance of available devices seems insufficient for sequential access (Table 1); parsing of incoming packets is heavily time-consuming. Pseudo paralleling is strongly required. This solution we used only in offline system implementation or when the internet connection is not available. In online (to the internet connected) system we send RAW (unparsed) data to the web service, which calls stored procedure for bitwise oriented parsing on database server. This "outsourced" data parsing is in a 12-chanel ECG measurement case faster as internal parsing, when is device unusable for overflow reason.

Table 1. Mobile Devices with LCD 480x800 pixels, GSM, WiFi, BT

Mobile device	OS WM	Display	CPU [Mhz]	SPB Benchmark Index
HTC Touch HD	6.1 Pro	LCD 3,8"	528	553
HTC Touch HD2	6.5 Pro	LCD 4,3"	1000	779
HTC Touch Diamond 2	6.5 Pro	LCD 3,2"	528	520
Samsung Omnia II	6.5 Pro	LED 3,7"	800	565

Table 2. BT ECG Device -> Mobile Device measurement

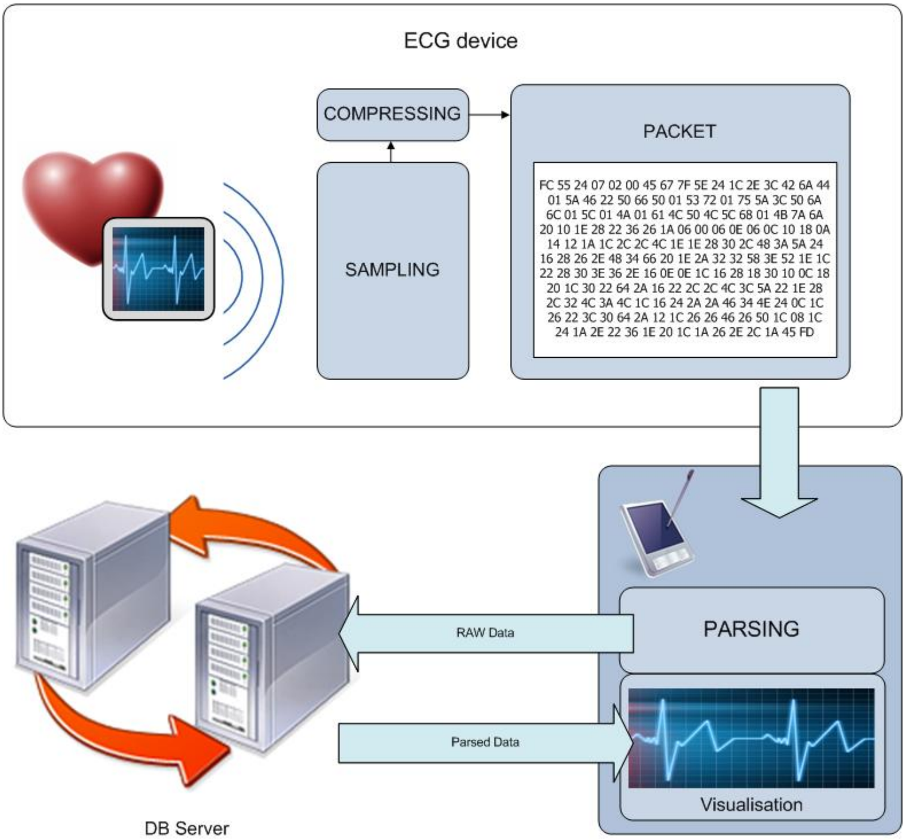
ECG device	Packet Size [Bytes]	Speed [Packets/s]	Transfer Speed [kB/s]
3 Channels	100	3x	0,3
12 Channels	300	5x	1,5

Table 3. BT ECG device measurement real-time packet parsing possibility

ECG device	Platform	Problem	Real Time
BT – Mobile device – Server – Visualization	.NET Framework	Memory overflow	Impossible
BT – Mobile device – Server – Visualization	C++	Memory overflow	Impossible
BT – Mobile device – Server – DB - Visualization	SQL Server procedure	-	Soft RT (2 sec deadline)
BT – MCU - Mobile device – Server - Visualization	MCU HCS08	-	Hard RT

4 Developed Hardware Parts of Platform

One of the main parts of system is a hardware background. If we want to analyze some data, we must measure and process it. This parts are realized over commercial ECG Corbelt, Blue ECG or own built ECG device for measurement and Cinterion AC75 GSM module for analysis (data parsing). GSM module is also used only in the own mobile device solution case.



```
FC 55 24 07 02 00 45 67 7F 5E 24 1C 2E 3C 42 6A 44
01 5A 46 22 50 66 50 01 53 72 01 75 5A 3C 50 6A
6C 01 5C 01 4A 01 61 4C 50 4C 5C 68 01 4B 7A 6A
20 10 1E 28 22 36 26 1A 06 00 06 0E 06 0C 10 18 0A
14 12 1A 1C 2C 2C 4C 1E 1E 28 30 2C 48 3A 5A 24
16 28 26 2E 48 34 66 20 1E 2A 32 32 58 3E 52 1E 1C
22 28 30 3E 36 2E 16 0E 0E 1C 16 28 18 30 10 0C 18
20 1C 30 22 64 2A 16 22 2C 2C 4C 3C 5A 22 1E 28
2C 32 4C 3A 4C 1C 16 24 2A 2A 46 34 4E 24 0C 1C
26 22 3C 30 64 2A 12 1C 26 26 46 26 50 1C 08 1C
24 1A 2E 22 36 1E 20 1C 1A 26 2E 2C 1A 45 FD
```

Fig. 2. Measurement, packet creating and packet parsing on mobile device schema

4.1 ECG Device

As measurement device is possible to connect several device with Bluetooth communication possibility. In our application we use an ECG Measurement Unit (bipolar ECG Corbelt or 12 channels BlueECG) through a virtual serial port using wireless Bluetooth technology.

The amount needed to transfer from source device through a Bluetooth is in Table 2. You can compare the increased data transfer speed in case of 12 channels ECG to 1 500 bytes per second. These data amount is very small; on the other hand the data are going as packets, so the processing is needed before the real data can be accessed.

This process (called "parsing") take an unacceptable time in case of mobile device to process the data in Real Time. Same problem is growing on desktop PC, where the C# or C++ is used. In both cases the Memory Overflow is reached. The only possible way we found is in use of SQL procedure which is executed on SQL server. When the data (packets) are stored in table the procedure is call to execute and provide RAW data. In such case the data are ready to user-consumer application until 2 second deadline, so the Soft Real Time is possible to use.

The RAW data table contains full size packets received from an ECG device. Only the packets with measured data are stored to database. Those packets must contain in part of packet number bytes with a value of 0x0724.

The table with parsed data contains decimal values. Column „I“ contains data from bipolar ECG; column „II“ with „I“ contains data from 6-channel ECG. The 12-channel ECG fills after parsing columns „I II V1 V2 V3 V4 V5 V6“.

To get a real ECG data immediately after the measurement the next way can be used. We can use a special microcontroller (MCU) embedded in USB unit. This MCU unit has a full speed (12Mbit/s) USB access and BT is connected through a serial port. The MCU unit process all needed operations with parsing to provide a real ECG record to database or directly to visualizing application. In case of WPF application the Hard Real Time mode was reached.

An example of real ECG record is shown in (Table 4) and (Table 5). In these cases, only Soft Real Time mode was reached even when a special MCU unit was used for preprocessing of data. In next subsection the use of WPF application is described as only way when the hard Real Time was reached on windows desktop PC (Windows RTX extension was used).

Table 4. Stored RAW data from ECG device in database table

id	RAW data	usr_id	Stamp	parsed
5238	0xFB3708000...EAC2FDC	13	5.1.2010 12:42:33.45	1
5239	0xFB284A000...0BB7EDC	13	5.1.2010 12:42:33.45	1
5240	0xFB2A3C000...40EA4DC	13	5.1.2010 12:42:33.45	1
5241	0xFB2846000...0DBAEDC	13	5.1.2010 12:42:33.45	1
5242	0xFB2893000...0CB8EDC	13	5.1.2010 12:42:33.45	1
5243	0xFB374B000...4A92FDC	13	5.1.2010 12:42:33.45	1
5244	0xFB2B5D000...80DA2DC	13	5.1.2010 12:42:33.45	1

Table 5. Parsed RAW data stored in database table

id	I	II	V1	V2	V3	V4	V5	V6	original_id
304	9250	7934	8163	5422	5743	8924	7365	8067	10102
305	7932	7396	8534	5709	6108	6385	6313	5893	10102
306	12520	8298	7446	8462	9032	7026	6359	7204	10102
307	7552	6580	6476	7243	9834	8549	7936	6228	10103
308	8976	5783	6948	9684	5638	9336	9316	9746	10103
309	9298	6224	9682	6734	5784	6164	5652	7046	10103
310	9114	9463	7466	4624	8256	9032	8552	8592	10104
311	9773	6350	7581	8779	7365	7231	5137	7295	10104
312	8627	6278	5274	5624	8645	7405	5874	6808	10104

4.2 Battery Consumption Tests

During the real tests the battery consumption tests were executed. Firstly the set of two monocell battery with nominal voltage of 2,5 V were tested without successful time of usage. They provide only 2 hours of operation time. At second case the Lithium-Polymer cell was used with nominal voltage of 3,7 V. In this case an additional circuitry is needed to use an USB port for recharging of battery in device. At figure (Fig. 3) the battery test screen of 12 channels ECG is presented. Figure shows the voltage of 3V (discharged battery) where current is presented by light trace on oscilloscope screen and its average value is approximately equal to 106 mA.

Figure (Fig. 4) shows the same at a normal charged battery voltage level where the average current is going down to 81 mA. In case of Li-Pol battery usage the operation time of 12 channels ECG is about 10 hours.

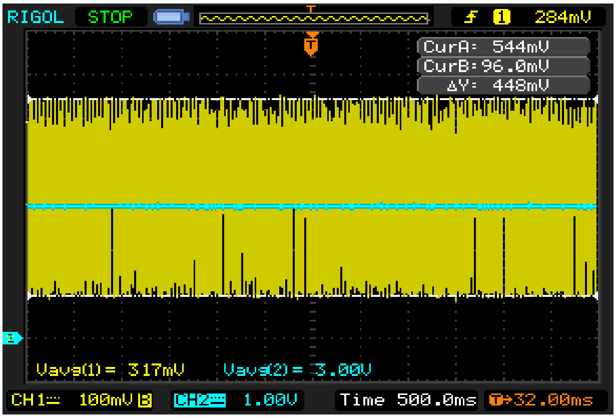


Fig. 3. Battery test screens of 12 channels ECG. Discharged battery.

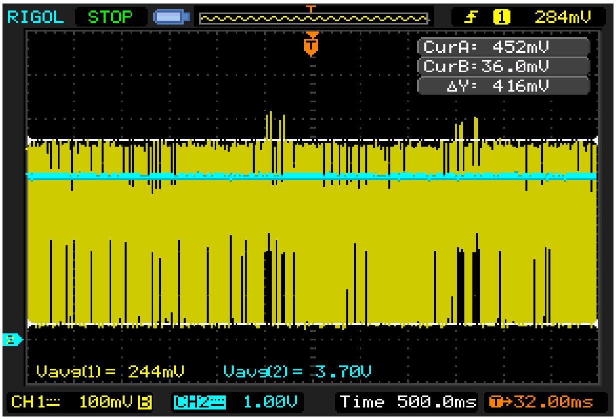


Fig. 4. Battery test screens of 12 channels ECG. Charged battery.

4.3 MCU Module and GSM Module

Other solution of parsing problem is a Java application in GSM module. The GSM module cointains own GSM communication module and processor which could be programmed by Java. The consumption of this microprocessor is acceptable, when we equals it to computing performance. Integrated processor have good computing power in bitwise operations, then the visualization application have to more time for own visualization. This is the same solution as special USB Bluetooth dongle with MCU. In other case is possible to the processed data append an informations about GPS position or data from accelerometer to visualize or send position data to user or

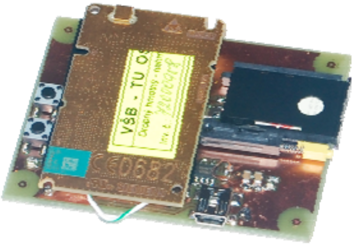


Fig. 5. Purpose-build GSM module

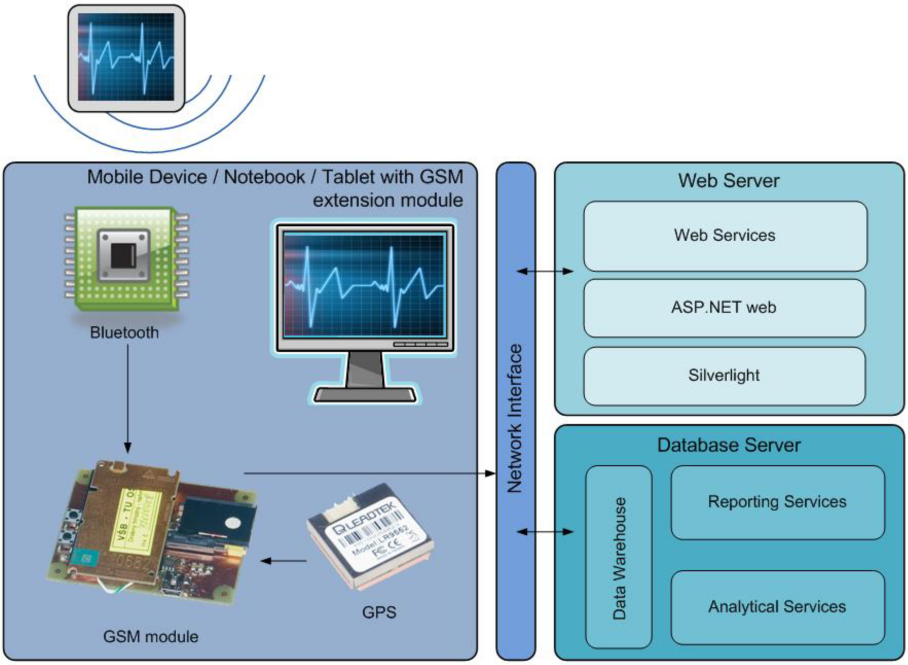


Fig. 6. Communication architecture

patient keeper eg. The special USB Bluetooth dongle consists in the construction of its way "smart" bluetooth module, which, in addition to its own communication interface also included a small single-chip microcomputer (MCU) with no operating system to work according to an algorithm for parsing mentioned packages and working as a parser.

Program in the MCU would work with individual bytes in the packet at the lowest hardware level, which should cause that for these operations will be sufficient very simple, small and inexpensive system with negligible energy demands. Both solutions takes place reliably in real time, and the parser could be equipped with a large enough flash memory cache. This could save the processed data at a time when it is not normal Real-Time operating system was unable to read and save. This would ensure that there is, in short-term 'freeze' the system is no loss of valuable data.

For the soft-real-time solution is here option, send data directly via GSM module to database server and use the stored parsing procedure particularly described in (section 3.1.).

5 User Interface Designing

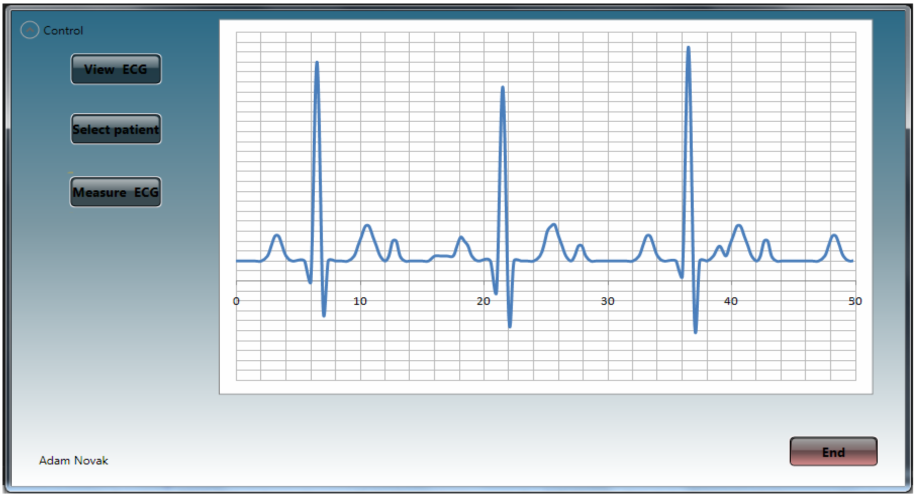
Proposal for this UI cyclically through several steps:

- Needs Analysis
- Design of UI
- Implementation of UI design and dynamics
- Testing

This is the so-called spiral development model, in which each spiral passage assess emerging requirements identified during testing of the current UI. At the very beginning of the development of UI, we have addressed a number of potential users. Questionnaires were sent to those under which we created the initial list of core requirements for the application and its UI. After the design and implementation of the application was sent back to users (in this case and inexperienced - viz. Testing UI). For testing, we obtained a list of comments on the application of its control and in some cases, suggestions of possible vylepšení.V this case, the tester user because our priority was to create such a UI, which is adapted to the user so that he worked well with him. Currently the application is again in the testing phase (4th course of the cycle) and in the near future we expect the results and any proposals for possible changes.

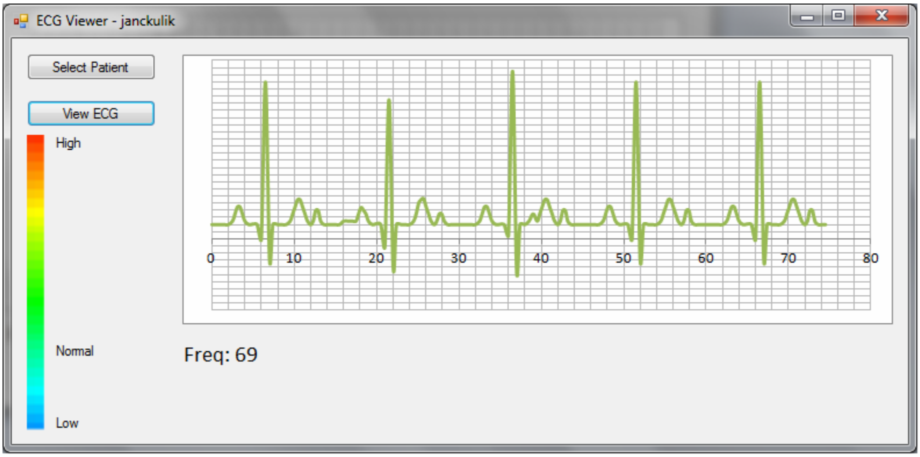
5.1 Visualization

To make an ECG visualisation the measured data are needed at the beginning. The measurement is made on bipolar ECG corbel and 12 channels BlueECG.



Adam Novak

Fig. 7. WPF ECG visualization application

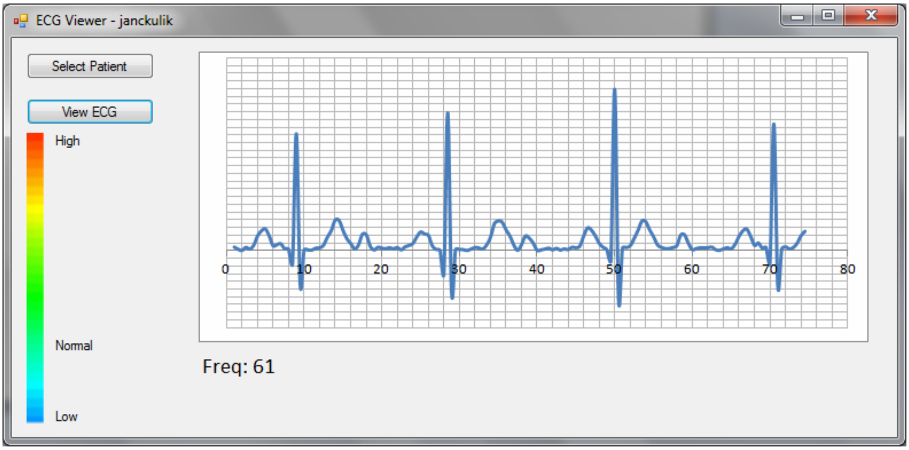


Freq: 69

Fig. 8. UA highlighting via the ECG curve color (normal pulse)

5.3 ECG Visualization in WPF Application

WPF (Windows Presentation Foundation) provide up to date possibilities to visualize ECG data on desktop PC. We create a WPF application to provide a full scale of graphic features to user. WPF technology runs directly on GPU possibilities (Graphic Processing Unit) which is founded on modern graphics cards. This fact is key parameter for speed of data presentation of screen. CPU has more time to compute others tasks (e.g. ECG data analyses by neural network tasks). WPF has a more



Freq: 61

Fig. 9. UA highlighting via the ECG curve color (elevated pulse)

design possibilities in compare to classical Windows Forms including 3D animation,pattern changes of whatever elements etc. WPF application allows viewing an ECG characteristic of measured patient in Real Time, selection of patient from database and view of historical graphs. The figure (Fig. 7) shows an example of bipolar ECG characteristic in WPF application.

6 User Interface Testing

To see our response to user created user interfaces, the application was submitted by fifteen users, divided into three groups according to their degree of user knowledge. Groups are "experienced user", "moderately experienced" and "Inexperienced user". Each user in the UI test assessed three aspects: friendliness, intuitiveness and overall rating. The user-friendliness of judging shows how he liked the graphic design of the program. Intuitiveness describes whether the user explore just guess what to do at that moment. The overall user evaluation of grades describes how he liked the overall application.

The results (Table 6) show that among users who are not accustomed to using similar applications and advanced user, there are only minimal differences. The worst rating of "4" has been achieved in a single user. It was inexperienced user reviews and intuitiveness. Second worst rating of "3" was obtained from a single user type "Inexperienced user", also in the evaluation of intuitiveness. Other users have always evaluated the application of the mark "1" and "2". Overall, all users have responded to the application well, had a problem with its use and its appearance and evaluated as friendly.

Table 6. User Adaptivity classification

Type of User	Assessment of user interface			
	Pleasantness	Intuitiveness	Response time	Summary
Inexperienced 1	1	2	2	1
Inexperienced 2	1	3	2	2
Inexperienced 3	2	1	2	2
Inexperienced 4	1	4	1	3
Inexperienced 5	1	1	1	1
Moderately experienced 1	2	2	2	2
Moderately experienced 2	1	1	1	1
Moderately experienced 3	1	1	1	1
Moderately experienced 4	1	1	2	1
Moderately experienced 5	1	3	1	2
Experienced 1	1	1	1	1
Experienced 2	2	1	1	1
Experienced 3	1	2	1	1
Experienced 4	1	1	1	1
Experienced 5	1	1	1	1

Table 7. Legend to user adaptivity classification

assessment	meaning
1	excellent
2	good
3	may be
4	bad

7 Conclusions

One of the most important parameters in the selection of applications has recently become a consumer society in the user interface. That´s why, in our applications we try to apply as much knowledge and available technology processes for their implementation. The measuring device (bipolar Corbelt ECG and 12 channels

BlueECG) which was tested in extreme conditions in a cryogen room in spa Teplice nad Becvou (Czech Republic) (-136°C), other design features in visualization software on outdoor device must be implemented. For these devices, (with Windows CE operating system) so powerful development tools for easy implementation are not available; as for indoor devices with operating systems clearly specialized for UI design (e.g. iPhone OS). The solution or the simplest way for implementation "handsome" UI for those "oldiest" devices with Windows CE is Microsoft Silverlight technology which is possible startup on Windows CE devices. The visualization of the measured data was reached in case of WPF usage. On the other side, for hardware parts the most important thing is the longest possible battery life for the longest operation time for measurement. Executed battery consumption tests provide a suggestion to use a Li-Pol battery with nominal voltage of 3,7 V. In such case the operation time is going to sufficient 10 hours. As the final improvement in the future, the application would have some special algorithm, which could recognize any symptoms of the QRS curve, and make the job for the doctors much easier.

Acknowledgment. This work was supported by the Ministry of Education of the Czech Republic under Project 1M0567.

References

1. Janckulik, D., Krejcar, O., Martinovic, J.: Personal Telemetric System – Guardian. In: Biodevices 2008, Insticc Setubal, Funchal, Portugal, pp. 170–173 (2008)
2. Krejcar, O., Cernohorsky, J., Janckulik, D.: Portable devices in Architecture of Personal Biotelemetric Systems. In: 4th WSEAS International Conference on Cellular and Molecular Biology, Biophysics and Bioengineering, BIO 2008, Puerto De La Cruz, Canary Islands, Spain, December 15-17, pp. 60–64 (2008)
3. Krejcar, O., Cernohorsky, J., Czekaj, P.: Secured Access to RT Database in Biotelemetric System. In: 4th WSEAS Int. Conference on Cellular and Molecular Biology, Biophysics and Bioengineering, BIO 2008, Puerto De La Cruz, Canary Islnds, Spain, December 15-17, pp. 70–73 (2008)
4. Krejcar, O., Cernohorsky, J., Janckulik, D.: Database Architecture for real-time accessing of Personal Biotelemetric Systems. In: 4th WSEAS Int. Conference on Cellular and Molecular Biology, Biophysics and Bioengineering, BIO 2008, Puerto De La Cruz, Canary Islands, Spain, December 15-17, pp. 85–89 (2008)
5. Krejcar, O., Janckulik, D., Motalova, L., Kufel, J.: Mobile Monitoring Stations and Web Visualization of Biotelemetric System - Guardian II. In: Mehmood, R., et al. (eds.) EuropeComm 2009. LNICST, vol. 16, pp. 284–291. Springer, Heidelberg (2009)
6. Krejcar, O., Janckulik, D., Motalova, L.: Complex Biomedical System with Mobile Clients. In: Dössel, O., Schlegel, W.C. (eds.) The World Congress on Medical Physics and Biomedical Engineering, WC 2009, Munich, Germany, September 07-12. IFMBE Proceedings, vol. 25/5, Springer, Heidelberg (2009)
7. Krejcar, O., Janckulik, D., Motalova, L., Frischer, R.: Architecture of Mobile and Desktop Stations for Noninvasive Continuous Blood Pressure Measurement. In: Dössel, O., Schlegel, W.C. (eds.) The World Congress on Medical Physics and Biomedical Engineering, WC 2009, Munich, Germany, September 07-12. IFMBE Proceedings, vol. 25/5. Springer, Heidelberg (2009)

8. Penhaker, M., Cerny, M., Martinak, L., Spisak, J., Valkova, A.: HomeCare - Smart embedded biotelemetry system. In: World Congress on Medical Physics and Biomedical Engineering, Seoul, South Korea, August 27-September 01. PTS 1-6, vol. 14, pp. 711–714 (2006)
9. Brida, P., Duha, J., Krasnovsky, M.: On the accuracy of weighted proximity based localization in wireless sensor networks. In: Personal Wireless Communications. IFIP, vol. 245, pp. 423–432 (2007)
10. Cerny, M., Penhaker, M.: Biotelemetry. In: 14th Nordic-Baltic Conference an Biomedical Engineering and Medical Physics, Riga, Latvia, June 16-20. IFMBE Proceedings, vol. 20, pp. 405–408 (2008)

Complex Mobile User Adaptive System Framework for Mobile Wireless Devices

Ondrej Krejcar

VSB Technical University of Ostrava, Center for Applied Cybernetics,
Department of measurement and control, 17. Listopadu 15,
70833 Ostrava Poruba, Czech Republic
Ondrej.Krejcar@remoteworld.net

Abstract. Paper describes a concept of User Adaptive System (UAS) as well as Predictive Data Push Technology (PDPT) Framework and Biotelemetrical Monitoring System (BMS) as two joined parts of complex UAS framework. Main focus is in contribution of UAS to user or patient and his life quality. A Position Oriented Database on a server and mobile devices is described as important part of whole UAS, because the position and context of user are one of the most important areas of UAS. Also the problem of low data throughput on mobile devices is described, which can be solved by PDPT framework. Localization and user tracking is described only as a necessary condition for prebuffering realization because the PDPT Core makes a decision when and which artifact (large data files) need to be prebuffered. Every artifact is stored along with its position information (e.g. in building or larger area environment). The accessing of prebuffered data artifacts on mobile device improve the download speed and response time needed to view large multimedia data. The conditions for real stocking in corporate areas are discussed at the end of paper along with problems that must be solved before stocking.

Keywords: User Adaptive System, Mobile Device, Localization, Biotelemetry, Position Oriented Database, Prebuffering.

1 Introduction

The idea of User Adaptive Systems (UAS) grown from interaction between user and system (e.g. throws his mobile device). Such interaction can behold in the reaction on user's non declared requests. These requests are based on current user environment and biological or emotional state (e.g where I am?, what I feel?, am I ok?, etc.). Such user questions can be answered by sensors on user body or inside the user devices. By the help of user mobile device, we can get a user location (e.g. user current position, user future-predicted position, his movement and tracking, etc.). Biomedical sensors on user body can detect several important biomedical data, which can be used for determination of user emotional state in the environment around.

By the combination of user’s requests (known or predicted) in conjunction with other sources of user’s knowledge and behaviors, the sophisticated information system can be developed based on presented UAS Framework.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 739–754, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

The impact of UAS can be seen in the increased user comfort when accessing these mobile UAS. In ideal case, everything what user can imagine to have in his mobile UAS is there.

A one specific kind of problems is based in increased data amount in new mobile systems. In current cases, the user need to specify a data to be downloaded to his mobile device and he need to wait for data downloading and displaying. Due to a several limitations in hardware of current mobile devices, the use of such large amount data has result in lower user comfort. The needs of any techniques to reduce such large data amount or to preload them before user's needs, is still growing up. We created a Predictive Data Push Technology (PDPT) Framework to solve these problems by data prebuffering. Our idea can be applied on a variety of current and future wireless network systems. More usability of PDPT grows from definition of area to be prebuffered as well as from evaluation of artifacts or other user's behavior sources. Additional will be presented in sections (3), (6).

The second area of problems which we would like to solve is based on a users biomedical data inputs and a wide area of their possible utility. Current body sensors allow a monitoring of a huge number of biomedical data information (e.g. use a special t-shirt equipped with an ECG, temperature, pressure or pulse sensors). Current hi-tech mobile devices are equipped with a large scale display, provide a large memory capabilities and a wide spectrum of network standards plus embedded GPS module (e.g. HTC Touch HD, HD2). These devices have built-in also a special accelerometer which can be used to determine a user's body situation (user is staying or lying). Last but not least equipment is a light sensor which can be used not only to brightness regulation. Use of these declared inputs will be discussed and presented in section (4).

2 Architectural Design for Ubiquitous Computing Systems

Ubiquitous Computing (UbiCom) is used to describe ICT (Information and Communication Technology) systems that enable information and tasks to be made available everywhere, and to support intuitive human usage, appearing invisible to the user [1].

Three basic architectural design models for UbiCom system can be divided to smart devices, smart environment and smart interaction. The concept of "smart" means that the object is active, digital, networked, can operate autonomously, is reconfigurable and has a local control of the resources which it needs such as energy, data storage, etc [1]. These three main types of system design may also contain subsystems, sub-parts or components at a lower level of granularity that may also be considered as a smart (e.g., a smart environment device may contain smart sensors and a smart controller, etc). An example of a three main types of UbiCom models is presented in (Fig. 1).

Many sub-types of smarts for each of the three main types of smarts can be recognized (Fig. 2). These main types of smart design also overlap between. Smart device can also support some type of smart interaction. Smart mobile device can be used for control of static embedded environment devices. Smart device can be used to support the virtual view points of smart personal spaces (physical environment) in a personal space which surrounding the user anywhere.

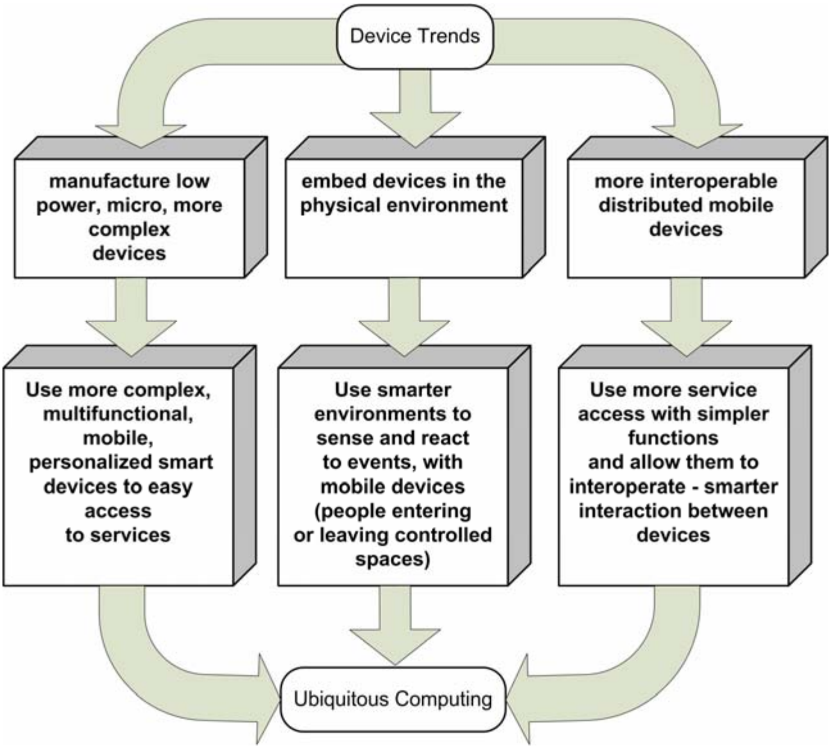

Device Trends
manufacture low power, micro, more complex devices
embed devices in the physical environment
more interoperable distributed mobile devices
Use more complex, multifunctional, mobile, personalized smart devices to easy access to services
Use smarter environments to sense and react to events, with mobile devices (people entering or leaving controlled spaces)
Use more service access with simpler functions and allow them to interoperate - smarter interaction between devices
Ubiquitous Computing

Fig. 1. Three models of ubiquitous computing: smart devices, smart environments and smart interaction [1]

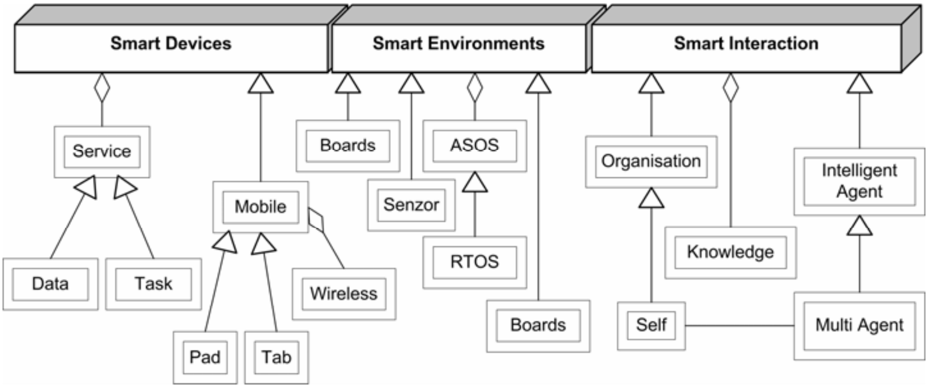


Fig. 2. Selected main subtypes of smart devices, environments and interactions including main aggregations between them. (MTOS is a Multi-Tasking Operating System, VM is a Virtual Machine, ASOS is an Application Specific or embedded system OS, RTOS is a Real-Time OS and MEMS is a Micro Electro Mechanical System) [1].

Satyanarayanan [3] has presented different architectures for developing UbiCom systems in way of which angle it is focused on a design:

1. Mobile distributed systems are evolved from distributed systems into ubiquitous computing
2. UbiCom systems are developed from smart spaces characterized by invisibility, localized scalability and uneven conditioning.

Poslad [1] has extended a Satyanarayanan model to Smart DEI model (Device Environment and Interactions). Poslads model also incorporates smart interaction. Smart DEI model also reverses to hybrid models (Fig. 2). It is widely assuming by users that the general purpose of end-user equipment will endure but also it will evolve into a more modular form.

2.1 Smart Devices

A smart device is a device that is digital, active, networked, user reconfigurable and that can operate to some extent autonomously. Smart devices can be characterized like personal computers or mobile phones with tend to be multi-purpose ICT devices. These devices operate as single portals used to access a multiple application services which are running locally on the device or remotely on servers. A range of forms are available for smart devices. Smart devices can be defined as personal devices, having a specified owner or user. In the smart device model, the place of application user interface is on side of the smart device. The main characteristics of smart devices consist of concept of: mobility, dynamic service discovery and intermittent resource access.

2.2 Smart Environments

A first definition of a smart environment brought by Coen [4] as a computation which is easily used to enhance ordinary activities. Cook and Das [5] refer to a smart environment as ‘one that is able to acquire and apply knowledge about the environment and its inhabitants in order to improve their experience in that environment’. A smart environment consists of a set of networked devices that have some connection to the physical world. The devices which are used for a smart environment usually execute a single predefined task (e.g., motion or body heat sensors coupled to a door release and lock control). Embedded environment components can be designed to automatically respond to interaction with user using iHCI (implicit Human Computer Interaction). A person can for example walk towards closed doors, which are automatically opens as a respond. By this reason the smart environments support a bounded, local context of user interaction. Smart environments will also follow a novel and revolutionary upgrades to be incorporated into the environment in the sense of a support less obtrusive interaction (pressure sensors can be for example incorporated into surfaces to detect a people sitting location or walking over).

2.3 Smart Interaction

While a smart devices and smart environments support the core properties of UbiCom, an additional type of design is needed to connect together their numerous particular activity interactions. Smart interaction is needed to support interaction model between UbiCom applications and their UbiCom infrastructure, physical world and human environments. In the smart interaction design model, system components dynamically interact to reach common goals. Components interact to reach goals jointly because they are deliberately not designed to execute and complete sets of tasks to reach goals all by themselves. There are several benefits to designs based upon sets of interacting components. Interaction between UbiCom system components does not exist only in one predefined level but it is spread in a range of levels from primitive to smart. Primitive interaction uses fixed interaction protocols between two statically linked dependent objects. While the smart interaction uses richer interaction protocols between multiple dynamic independent objects.

2.4 Adaptive Systems for Ubiquitous Computing

Ubiquitous computing provides a vision of computing systems which are located everywhere around us, embedded in the things of our everyday life. They provide an easy access to information and communications bases dedicated to our current location. People are able to interact with any ubiquitous computing environment which they attend. This is a reason why the ubiquitous computing environments must respond dynamically to specific user needs, resources dedicated to their owner's rights or to the current usage context. These require a high level of adaptivity which must be provided by ubiquitous computing systems and related connecting networks [2].

Described project deals with several of issues related to providing such adaptivity for ubiquitous computing environments which will be described more in the following sections.

3 Reaction on a Change of Location – Location-Aware Adaptation

We can imagine the usage of such described UAS in the information systems area of botanical or zoological gardens. In such areas there has been a big potential of usage of a continual localization by use of GPS or wireless networks (in case the GPS has not a sufficient signal – e.g. in urban centers or neighborhoods with high buildings, forest parks or in deep valleys). There is also a possibility to compute a current and predicted user track, so we can predict a position of user in near future (e.g. 25 meters north in one minute). Usability of these information sources is uncountable.

One of possible use of user predicted position is for a determination of a data, which will be needed by user of mobile UAS in near future. Such data (data artifacts) can be preloaded to user's device memory for future requests. The need of preloaded artifacts grown from a need of up to date data context of dynamic online system. Of course when static offline system is used, there is a possibility to load a needed data before usage (e.g store artifacts at SD Card with a size limit to several GB). When user request info about his location in context of zoo or garden (turn-on the device is only needed by user), the client application will respond with a map of near surroundings and a prebuffered data artifacts. User can select a documentary about animals or vegetation around him which can be viewed or played. User can act with direct requests to selected kinds of these. These preferred kinds will be taken into account to evaluate future objects/artifacts and preloaded only the most important ones for a user. The type of artifact is also evaluable as well as his size because the user may not want to look at too long or micro presentation. xxxxxxxx

As client devices of online UAS, the mobile wireless devices like PDA or Smart phones are commonly used equipped with internet connectivity. The connection speed of the two most common standards GPRS and WiFi varies from hundreds of kilobits to several megabits per second. In case of online UAS or some other types of facility management, zoological or botanical gardens, libraries or museums information systems, the WiFi infrastructure network is often used to interconnect mobile device clients with a server. Unfortunately, the low performance hardware components are used in PDAs or SmartPhones due to a very limited space. Due this a theoretical maximum connection speed is not reachable on such devices. The limited connection speed represents a problem for clients of online system using large artifacts (data files). In some specific cases it is not possible to preload these artifacts before the use of mobile device in a remote access state due any reason.

3.1 Low System Throughput on Current Mobile Devices

The real downlink speed for WiFi network (802.11b,g) is about 1280 kbit/s for modern PDA devices [7], [8], [9]. Primary dataflow can be increased by data prebuffering. Selecting of data objects to be buffered to mobile device cache is made on the base of position of user's device. For every position in area, where the prebuffering is being made, the location-aware objects for such user's position exists. PDPT Core pushes a data from SQL database (WLA database (Fig. 3)) to clients PDA on a base of PDPT Core decision algorithm.

The benefit of using a PDPT consists in reduction of time delay, which is needed to display requested artifacts from PDA client. This delay must not be longer than the time for which a user is able to wait for some response from application. Hence, the maximum response time of an application (PDPT Client) for user must be specified firstly. Nielsen in his book [10] specified this time delay to 10 seconds [11]. During this time the user was focused on the application and was willing to wait for an answer. The Nielsen book is a basic literature for this phenomenon. Galletta, Henry, McCoy and Polak (2002) findings suggest that, 'decreases in performance and behavioral intentions begin to flatten when the delays extend to 4 seconds or longer, and attitudes flatten when the delays extend to 8 seconds or longer'.

Based on this knowledge, we defined this delay for our testing purposes to 5 seconds. For this time is possible to transfer (from server to client) a data amount of 800 kB (for 1280 kbit/s downlink).

The next step was an average artifact size definition. The network architecture building plan is used as a sample database, which contained 100 files of average size of 470 kB. The client application can download during the 5 second period from 1 to 2 artifacts. The final result of several real tests and consequential calculations is definition of artifact size to average value of 500 kB. The buffer size may differ from 50 to 100 MB in case of 100 to 200 artifacts.

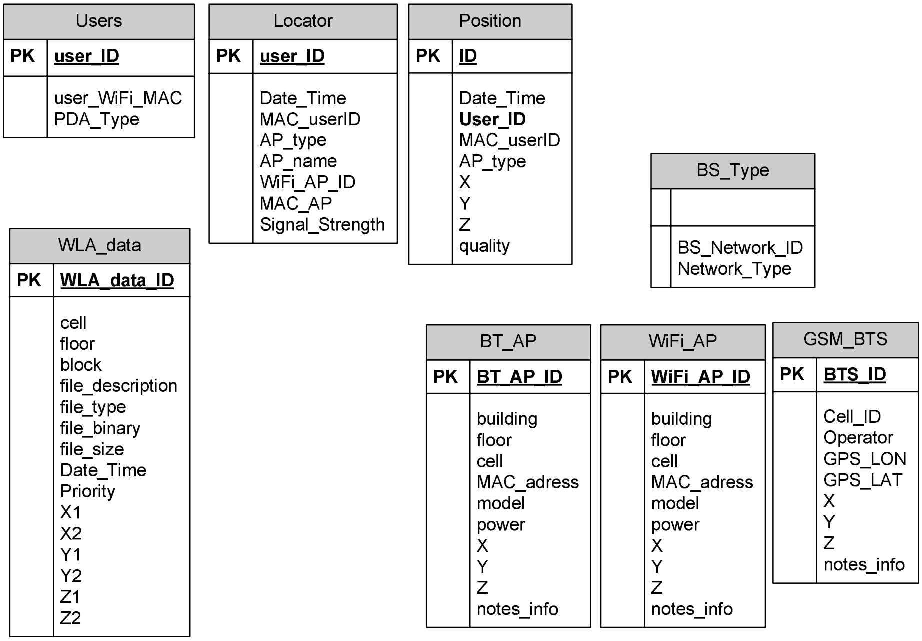
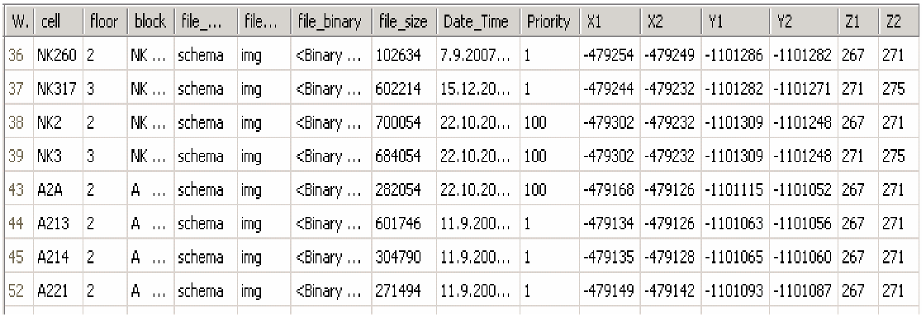


Fig. 3. Scheme of WLA architecture (Wireless Location Architecture) PDPT server database

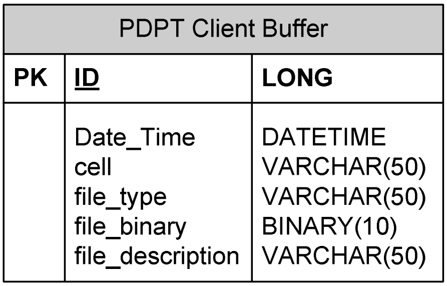
3.2 Position Oriented Database

If the mobile device knows the position of the stationary device (transmitter), it also knows that its own position is within a range of this location provider [6], [12]. The typical range varies from 30 to 100 m in WiFi case, respectively 50 m in BT case or 30 km for GSM. Granularity of location can be improved by triangulation of two or more visible APs (Access Points) or using the more accurate position algorithms (Monte Carlo localization). In PDPT framework only the triangulation technique is used due to the sufficient granularity of user position information. Monte Carlo localization was tested in one segment of tested environment without marginal success

Table 1. PDPT Server – SQL Server 2005 database – *WLA_data* table



W.	cell	floor	block	file_...	file...	file_binary	file_size	Date_Time	Priority	X1	X2	Y1	Y2	Z1	Z2
36	NK260	2	NK ...	schema	img	<Binary ...	102634	7.9.2007...	1	-479254	-479249	-1101286	-1101282	267	271
37	NK317	3	NK ...	schema	img	<Binary ...	602214	15.12.20...	1	-479244	-479232	-1101282	-1101271	271	275
38	NK2	2	NK ...	schema	img	<Binary ...	700054	22.10.20...	100	-479302	-479232	-1101309	-1101248	267	271
39	NK3	3	NK ...	schema	img	<Binary ...	684054	22.10.20...	100	-479302	-479232	-1101309	-1101248	271	275
43	A2A	2	A ...	schema	img	<Binary ...	282054	22.10.20...	100	-479168	-479126	-1101115	-1101052	267	271
44	A213	2	A ...	schema	img	<Binary ...	601746	11.9.200...	1	-479134	-479126	-1101063	-1101056	267	271
45	A214	2	A ...	schema	img	<Binary ...	304790	11.9.200...	1	-479135	-479128	-1101065	-1101060	267	271
52	A221	2	A ...	schema	img	<Binary ...	271494	11.9.200...	1	-479149	-479142	-1101093	-1101087	267	271



PDPT Client Buffer		
PK	**ID**	**LONG**
	Date_Time	DATETIME
	cell	VARCHAR(50)
	file_type	VARCHAR(50)
	file_binary	BINARY(10)
	file_description	VARCHAR(50)

Fig. 4. PDPT Client – SQL Server 2005 Mobile Edition database – *Buffer* table

(Time needed to implement algorithm was inadequate to position quality results). Information about the user position are stored in *Position* table (Fig. 3). *Locator* table contain info about wireless AP with signal strength which are needed to determine user position. *WiFi_AP, BT_AP* and *GSM_AP* tables contain all necessary info about used wireless base stations. *WLA_data* table contain data artifact along with their position, priority and others metadata.

3.3 PDPT Client - Mobile Database Server

The large data artifacts from PDPT Server (WLA_data table (Fig. 3), (Table 1)) are needed to be presented for user on mobile device. In case of classical online system the data artifacts are downloaded on demand. In case of PDPT solution, the artifacts are preloaded to mobile device cache before user requests. As mobile cache the SQL Server 2005 Mobile Edition was selected. Our mobile cache contain only one data table Buffer (Fig. 4). Only the needed columns from PDPT server WLA_data table were taken for mobile version Buffer table. MS SQL Server 2005 Mobile Edition was selected for easiest managing of them in case that the Visual Studio and classic SQL Server are used. Small data amount for installation (2,5 MB) is also an advantage.

4 Reaction on a Change of Biomedical Data – Active Context-Aware Adaptation

A key problem of context-aware systems design is to balance the degree of user control and awareness of their environment. We can recognize two extreme borders as active and passive context-aware. In active context-aware system, the UAS is aware of the environment context on behalf of the user, automatically adjusting the system to the context without the user being aware of it [1]. This is a useful in our application where a strict time constraints exists, because the user-patient cannot due to immobility, or would not otherwise be able to adapt to the context quickly enough.

We are using principles of UAS in area of biomedical data processing, where we try to predict some kind of problems by patient data analysis. We developed a context-aware Biotelemetrical Monitoring System (BMS) [13] as a part of the UAS and PDPT Framework project facilitates the following:

- Real-time collection of the patient vital signs (e.g. ECG, EEG) by means of a Body Area Network (BAN) or direct wireless connection to PDA device monitoring station.
- Real-time transmission of the vital signs using the wireless connectivity to the healthcare professionals through a complete architecture including a server database, web services, doctors web access to patients collected and preprocessed data.
- Seamless handover over different wireless communication technologies such as BlueTooth, WiFi, GPRS or UMTS.
- Context-aware infrastructure to sense the context (e.g. location, availability, activity, role) of the patients and Emergency Response Services (ERSs) to provide assistance to the patient in case of an emergency. An ERS could be fixed (e.g. hospital) or mobile (e.g. caregiver). A mobile ERS is published in the BMS.

Classical access to patients request are made by reactive flowchart (Fig. 5.a), where a patient is equipped with a classical offline measuring devices with some type of alarms. Every violated alarm need to be a carried out by doctor decision. Such access is very time-consuming.

Second proposed access is based on a proactive principle (Fig. 5.b), where the patient is equipped with an online measuring devices with an online connection to some

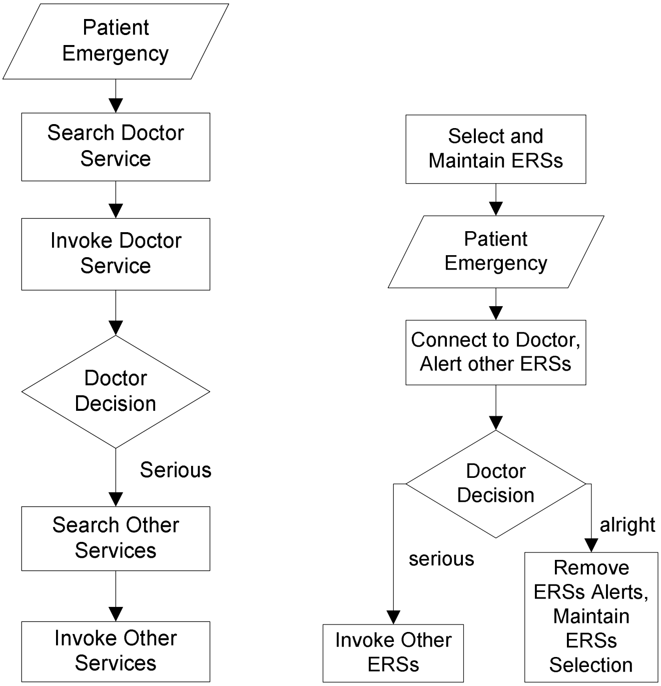


Fig. 5. Flowchart of Reactive (Left – Fig. 5.a) and Proactive (Right – Fig. 5.b) ERSs Selection and Invocation Approach.

kind of superior system (in our case the BMS is presented). In this case, a patient's measured data are processed on mobile monitoring station or at server. An alert will invoke when the anomaly data are founded in patient's records. Consequently the doctor is responsible to make a decision to invoke other ERSs or to remove Alarm (in case of false detection of anomaly). Such kind of behavior is based on UAS. In many of events a predicted and solved problems can save a life. The predicted patient's problems are in most cases minor in compare to a major problems detected in time where occurred.

4.1 Biomedical Data Acquisition, Processing and Proactive Reaction

Our developed BMS can currently handle two types of biomedical data:

- 12 channels wireless ECG – BlueECG (CorScience company)
- bipolar wireless ECG – corbel (CorScience company)

These data are measured, preprocessed on mobile monitoring station (PDA, embedded device, notebook), visualized on monitoring station's display (in available), sent by wireless connection to web service and stored on server for consequential access by doctors or medical personal. Used data acquisition devices provide a successful result in case of testing a developed solution. In near future we plan to use a t-shirt with equipped biosensors network (e.g. ECG, pulse, oxy, pressure).

The biomedical ECG data are continually processed (in Real Time) through a complete infrastructure of developed UAS. First false artifact recognition is made on mobile measurement stations near the patient to allow an immediate action from ERSs.

The more sophisticated data analysis is made at server level. This data processing is made on the base of neuron network and fuzzy logic behavior. Unfortunately, we reach only a small level of successful false detection (patient problem detection) up to date. In this area we are expected a future impact of our solution. The low detection rate is caused by several facts. Of course the better algorithms are needed at the first, but this problem cannot be solved satisfactory in near future. Another problem is caused by a slow connection by WiFi network, because some biomedical data contain a huge amount of data. This problem is possible to solve by our PDPT framework as a part of our UAS solution. By this solving, we improve the quality of detection by a 40 % (median value of 12 channels ECG). All the same, the real time transfer rate is now still fail to reach.

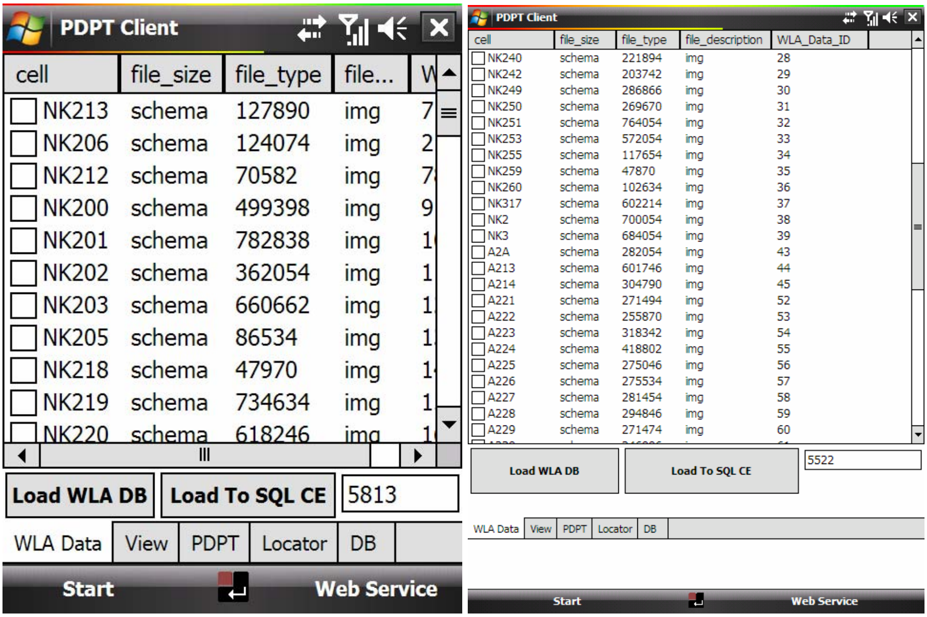
5 Reaction on a Change of Logged User – Personal-Aware Adaptation

Next possible way to react on user needs is in classical user input processing. Based on user login a personal-aware adaptation of UAS can be defined. Well known is a model of screen resolution adaptation based on a used mobile device. Classical way is in user setting module located in used application. This however requests a user action at each time a different user is logged in.

5.1 Adaptive User Interface for Mobile User Adaptive System

To prevent such waste user time, user interface adaptivity can be developed and used based only on user login information. UAS server can collect a user data such as a request of special user interface layout (font size, buttons size and locations, wide of scrollbars, etc.). After user login application is initiated in used best fitting scheme. Example of such user defined user interface is shown at (Fig. 6).

Depending on a user ability to view smaller fonts an indispensable number of other rows are viewable by user a higher resolution (Fig. 6).



cell	file_size	file_type	file...	W
☐ NK213	schema	127890	img	7
☐ NK206	schema	124074	img	2
☐ NK212	schema	70582	img	7
☐ NK200	schema	499398	img	9
☐ NK201	schema	782838	img	1
☐ NK202	schema	362054	img	1
☐ NK203	schema	660662	img	1
☐ NK205	schema	86534	img	1
☐ NK218	schema	47970	img	1
☐ NK219	schema	734634	img	1
☐ NK220	schema	618246	img	1

5813

cell	file_size	file_type	file_description	WLA_Data_ID
☐ NK240	schema	221894	img	28
☐ NK242	schema	203742	img	29
☐ NK249	schema	286866	img	30
☐ NK250	schema	269670	img	31
☐ NK251	schema	764054	img	32
☐ NK253	schema	572054	img	33
☐ NK255	schema	117654	img	34
☐ NK259	schema	47870	img	35
☐ NK260	schema	102634	img	36
☐ NK317	schema	602214	img	37
☐ NK2	schema	700054	img	38
☐ NK3	schema	684054	img	39
☐ A2A	schema	282054	img	43
☐ A213	schema	601746	img	44
☐ A214	schema	304790	img	45
☐ A221	schema	271494	img	52
☐ A222	schema	255870	img	53
☐ A223	schema	318342	img	54
☐ A224	schema	418802	img	55
☐ A225	schema	275046	img	56
☐ A226	schema	275534	img	57
☐ A227	schema	281454	img	58
☐ A228	schema	294846	img	59
☐ A229	schema	271474	img	60

5522

Fig. 6. User interface layout initiated based on UAS server data. QVGA layout on a VGA display (Left – Fig. 6.a) and VGA layout on same device (Right – Fig. 6.b)

5.2 New Components for Mobile User Adaptive Systems

However not every user is able to access small fonts so user interface with a large elements of user interface are welcome. Examples of such elements are described in (Fig. 7, 8, 9). A first example presents switchers (Fig. 7). They provide a sizable intuitive way to support an adaptation on user ability. Every described element is developed as components of UAS framework. Use in any other projects is therefore very easy and comfortable.

Another component of UAS framework is navigation arrows (Fig. 7.c.), which is a sizeable component with one enumeration type of direction which can be used to easily navigate in some outdoor use cases.

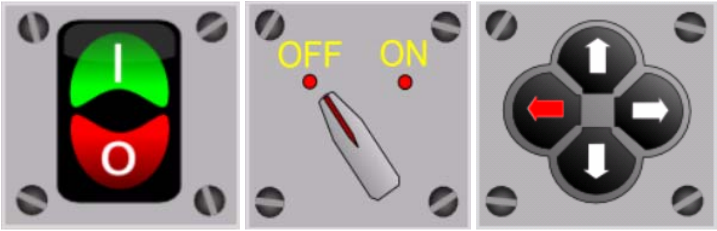


Fig. 7. User interface components: 0/1 switch (Left – Fig. 7.a), On/Off switch (Middle – Fig. 7.b) and navigation arrows where a left direction is selected (Right – Fig. 7.c)

Next component of UAS framework is circle visualizer (Fig. 8.a.), which is a sizeable component with two properties: color areas definition and min-max values. This component can be used to inform user about valued state of some controlled properties in the context of their boundary values. By use of this context a user can get more complex information instead of classical value information (e.g. in text/numerical form).

The last example of component is based on previous circle visualizer component, which is parent of a new component is sense of object programming model. The component can represent e.g. voltmeter (Fig. 8.b.) or milliammeter (Fig. 8.c.) as a two examples of measurement visualization component. From parent it inherits all properties and it adds a text properties for type of meter which it is represent in real case. Of course the shape is not a circle type, but it is rectangle.

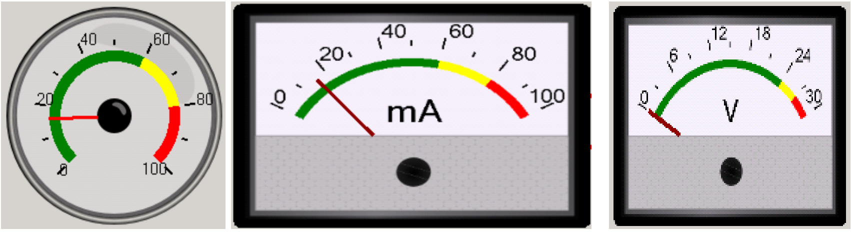


Fig. 8. User interface components of measurement visualization: value of 17 at circle visualizer (Left – Fig. 8.a), milliammeter (Middle – Fig. 8.b) and voltmeter (Right – Fig. 8.c).

6 The User Adaptive System Framework

A combination of a predicted user position with prebuffering of data, which are associated with physical location bears many advantages in increasing throughput of mobile devices. The key advantage of PDPT solution in compare to existing solutions [12], [13] is that the location processing, track prediction and cache content management are situated at server side. The solution allows for managing many important parameters (e.g. AP info changes, position determination mechanism tuning, artifacts selection evaluation tuning, etc.) online at a server. By adding a *Biomedical Data*

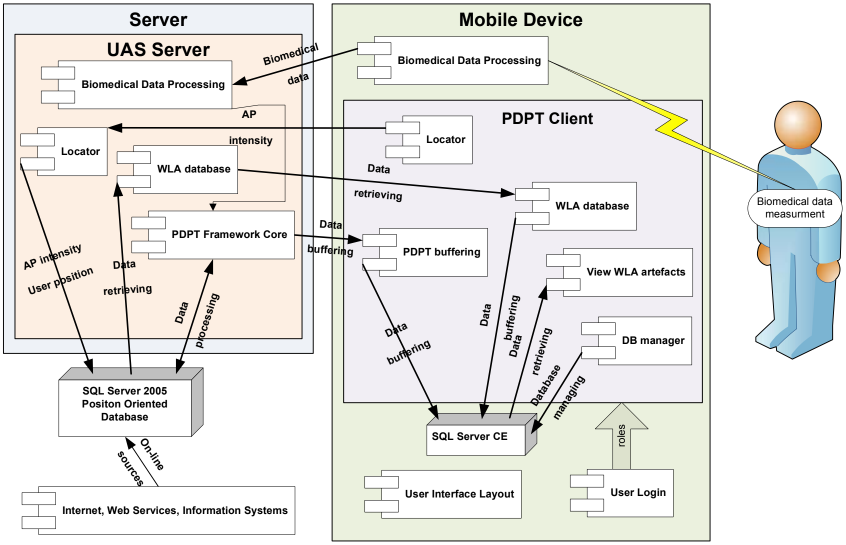


Fig. 9. User Adaptive System Framework architecture. Mobile device user is equipped with biotelemetry sensors to get info about user's body. User's mobile device has embedded WiFi connectivity, which is used in locator sensor component.

Processing solution, the Complex User Adaptive System (UAS) Framework is growing from (Fig. 10). While the whole PDPT Framework concept allow to manage a artifacts in context-awareness and time-awareness, the UAS Framework shift these possibilities to manage artifacts in biomedical context-awareness allowing a response for example to user´s non declared needs.

Biomedical Data Processing sensor at Mobile Device side of architecture (Fig. 10) collect information from user's body through a Bluetooth connection to any kind of wearable biotelemetrical devices. These data are transferred to UAS Server along with locator module data, which is processing these knowledge to act with adequate reaction in sense of user comfort improvement as a response time reducing for requested information by data prebuffering or any other reaction (e.g. screen resolution improvement, display brightness etc.).

Artifact data object can be defined as a multimedia file type in complex-awareness, which represent an object in Position Oriented Database – table *WLA_data* with time, position and biomedical-awareness. To manage locations of artifacts, firstly the building map is needed [15]. The position of corporate APs is also needed to determine a user position based on a distance from each visible APs [8], [12], [6]. All obtained positions info need to be stored in UAS server database through a PDPT Core web service. Artifacts with position coordinates are stored in *WLA_data* table (Table 1) by use of "WLA Database Artifact Manager". This software application was created to manage the artifacts in Position Oriented Database [8].

The PDPT prebuffering principle consists of several following steps:

1. Client must activate the PDPT buffering checkbox on PDPT tab at PDPT Client, which creates a list of artifacts (PDA buffer view sample which contain

only ID of artifacts), which are contained in his mobile SQL Server CE database.

2. PDPT Framework Core web service module creates own list of artifacts (imaginary view sample of PDA buffer) dedicated to actual user device position. It also compares it with real "PDA buffer view sample". The area is defined as a 3D rectangle object where the user's position is located in center.
3. The PDPT Core continues in next step with comparing of both images. If there are some missed artifacts in PDA buffer, they are prebuffered to PDA buffer. When all artifacts for current user position are prebuffered in PDA buffer, there is no difference between images.
4. After all artifacts are prebuffered to PDA buffer of mobile client, the PDPT Core is going to make steps 1 to 3 once more for a new predicted user position with new enlarged area (3D rectangle).

7 Discussion of Results

The PDPT Framework project is developed from 2005 until now in several consequential phases. Current state of the project is near the real company stocking. Final tests were executed in university campus of Technical university of Ostrava. For company stocking is possible to think about several areas. These possibilities will be discussed in [section 7.2].

7.1 Final Test Results of PDPT Framework Part

For testing purpose, five mobile devices were selected with different hardware and software capabilities. Six types of tests batches were executed in test environment. Two different test scenarios were executed as static and dynamic tests scenarios.

Static test was based on a predefined collection of data artifact which belongs to defined user position in test environment. Five test position were selected where approximately 12 data artifacts was needed to successful prebuffering. Three iterations were repeated in each position. If any of these expected artifacts stay un-buffered, the quality of prebuffering is going low. The tests were performed with result from 69,23 % to 100 %. The mean value of test results was 93,63 %. From all 15 tests, the 9 were executed with a 100 % of successful score.

Every dynamic test was between two points with 132 meter distance. Every even test was in reversed direction. Five iterations (five devices used) were made during one batch. Results provide a good level of usability when user is moving slowly (less than 0,5 m/s). This fact is caused by low number of visible WiFi APs in test environment, where 60 % of time only 1 AP was visible, 20 % for 2 visible and 5 % for 3 or more visible WiFi APs. 15 % of time represents a time without any WiFi connections. Reached values of prebuffering quality in such case are very good.

7.2 Possibilities of Using a PDPT Framework in Real Environment

Dynamic tests of PDPT Framework show the problem of a low number of visible WiFi APs for localization determination in the test environment of university campus. For the real case of usage and for the high level of prebuffering quality, the minimal number of simultaneously visible WiFi APs at each place of stocking area must be from 3 APs.

For successful stocking of PDPT, the area of prebuffering is needed to be defined and also the data artifacts must be defined. One way is in use of developed software “WLA Database Artifact Manager” for offline case, but the useful solution is in determination of large data objects in online case. Such determination is not easy. Possible solution can be seen in application of Position Oriented Database scheme to convert an existing server database of online system to Position Oriented Database structure. After such conversion, the data are possible to select based on position in stocking area. Consequently if data object – artifact can be selected, the PDPT server can prebuffer such data to mobile device.

As a summary, the PDPT is now usable at immobile patients at 100% successful rate of prebuffered artifacts. Such sort of patients is specific for only low speed of their transfer inside the environment. Due this fact the PDPT is functioning. If the environment for prebuffering will be equipped with a higher number of WiFi APs, the usability of PDPT in dynamic cases will be much more achievable.

8 Conclusions

A concept of UAS as well as PDPT Framework and BMS Framework was described with main focus on Position Oriented Database on server and mobile devices. Coexistence of proposed solutions is in unnumbered areas and the results of complex solution are better than expected. Also the final static and dynamic tests were performed and discussed. The developed UAS can be stocked on a wide range of wireless mobile devices for its main issue at increased downlink speed. The localization part of PDPT framework is currently used in another project of biotelemetrical system for home care agencies to make a patient’s life safer [13]. Several areas for PDPT stocking was founded in projects of Biotelemetry Homecare [14], [16]. In these selected areas the use of PDPT framework is not only partial, but complete include the use of wide spectrum of wireless communication networks and GPS for tracking people and urgent need of a high data throughput on mobile wireless connected monitoring devices. Several of UAS principles can be used there also. These possibilities will be investigated in future.

Acknowledgement This work was supported by the Ministry of Education of the Czech Republic under Project 1M0567

References

1. Poslad, S.: Ubiquitous Computing: Smart Devices, Environments and Interactions. John Wiley & Sons, Ltd., London (2009), ISBN 978-0-470-03560-3
2. Lewis, D., O’Sullivan, D.: Adaptive Systems for Ubiquitous Computing. In: Proceedings of the 1st international symposium on Information and communication technologies. ACM International Conference Proceeding Series, vol. 49, p. 156 (2003)
3. Satyanarayanan, M.: Pervasive computing: vision and challenges. IEEE Personal Communications 8, 10–17 (2001)

4. Coen, M.H.: Design principles for Inteligent environments. In: Proceedings of 15th National/10th Conference on Artificial Intelligence/Innovative Applications of Artificial Intelligence, pp. 547–554 (1998)
5. Cook, D.J., Das, S.K.: How smart are our environments? An updated look at the state of the art. Pervasive and Mobile Computing 3(2), 53–73 (2007)
6. Brida, P., Duha, J., Krasnovsky, M.: On the accuracy of weighted proximity based localization in wireless sensor networks. In: Personal Wireless Communications. IFIP, vol. 245, pp. 423–432 (2007)
7. Krejcar, O.: Prebuffering as a way to exceed the data transfer speed limits in mobile control systems. In: ICINCO 2008, 5th International Conference on Informatics in Control, Automation and Robotics, Funchal, Portugal, May 11-15, pp. 111–114 (2008)
8. Krejcar, O., Cernohorsky, J.: New Possibilities of Intelligent Crisis Management by Large Multimedia Artifacts Prebuffering. In: I.T. Revolutions 2008, Venice, Italy, December 17-19. LNICST, vol. 11, pp. 44–59. Springer, Heidelberg (2008)
9. Krejcar, O.: Problem Solving of Low Data Throughput on Mobile Devices by Artefacts Prebuffering. EURASIP Journal on Wireless Communications and Networking, Article ID 802523, 8 pages (2010)
10. Nielsen, J.: Usability Engineering. Morgan Kaufmann, San Francisco (1994)
11. Haklay, M., Zafiri, A.: Usability engineering for GIS: learning from a screenshot. The Cartographic Journal 45(2), 87–97 (2008)
12. Ramrekha, T.A., Politis, C.: An Adaptive QoS Routing Solution for MANET Based Multimedia Communications in Emergency Cases. In: MOBILIGHT 2009, Athens, Greece. LNICST, vol. 13, pp. 74–84. Springer, Heidelberg (2009)
13. Krejcar, O., Janckulik, D., Motalova, L., Kufel, J.: Mobile Monitoring Stations and Web Visualization of Biotelemetric System - Guardian II. In: Mehmood, R., et al. (eds.) EuropeComm 2009. LNICST, vol. 16, pp. 284–291. Springer, Heidelberg (2009)
14. Cerny, M., Penhaker, M.: Biotelemetry. In: 14th Nordic-Baltic Conference an Biomedical Engineering and Medical Physics, Riga, Latvia, June 16-20. IFMBE Proceedings, vol. 20, pp. 405–408 (2008)
15. Krejcar, O.: Full Scale Software Support on Mobile Lightweight Devices by Utilization of all Types of Wireless Technologies. In: Granelli, F., Skianis, C., Chatzimisios, P., Xiao, Y., Redana, S. (eds.) Mobilight 2009. LNICST, vol. 13, pp. 173–184. Springer, Heidelberg (2009)
16. Penhaker, M., Cerny, M., Martinak, L., Spisak, J., Valkova, A.: HomeCare - Smart embedded biotelemetry system. In: World Congress on Medical Physics and Biomedical Engineering, Seoul, South Korea, August 27-September 01. PTS 1-6, vol. 14, pp. 711–714 (2006)
17. Brasche, G.P., Fesl, R., Manousek, W., Salmre, I.W.: Location-based caching for mobile devices. United States Patent, Microsoft Corporation, Redmond, WA, US, 20070219708 (2007)
18. Squibbs, R.F.: Cache management in a mobile device. United States Patent, Hewlett-Packard Development Company, L.P., 20040030832 (2004)

The Indoor Orientation of Autonomous Mobile Devices for Increasing Human Perspective

Jiri Kotzian, Jaromir Konecny, Ondrej Krejcar, Tomas Lippa,
Hynek Prokop, and Marian Kuruc

VSB-Technical University of Ostrava, Department of Measurement and Control,
17. listopadu 15, 70833 Ostrava-Poruba, Czech Republic
`{jiri.kotzian,jaromir.konecny.st,ondrej.krejcar,`
`tomas.lippa.st,hynek.prokop.st,marian.kuruc.st}@vsb.cz`

Abstract. During recent years, rises in terrorist attacks and armed conflicts have increased the demand for autonomous devices. The need for devices with the ability to detect toxic gases, to be fire resistant and to multifunction has increased. We propose a concept of two such devices with the ability to comfortably and remotely control such devices and even with an autonomous control in remote areas inside the buildings. The localization by WiFi is used to locate a position where the GPS signal is not well presented. The ability to locate a mobile device by a wireless network is a well known possibility. Position information tools are currently used in many current areas. The main area of interest is in the use of locating and tracking users of a mobile information system to prebuffer large amounts of data to them before usage. All large data files are stored as artifacts along with its position information in a building or a larger area. The accessing of prebuffered data on mobile devices can highly improve response time needed to view large multimedia data. This fact can help with the design of new full scale applications for mobile devices.

Keywords: Orientation, Navigation, Embedded system, Wireless communication.

1 Introduction

The usage of mobile devices for orientation in open spaces has increased. There are several global navigation systems like GPS, Glonass etc. Navigation systems are very helpful in our everyday lives. The problem is rising in places with a high density of buildings. The precision of computing positions is too low. Inside buildings the navigation is usually not possible at all. The reason is low signal or total signal absence.

Different technologies for the navigation of mobile devices have to be used in buildings. For example: the human body uses stereovision for environment detection and orientation in cooperation with “maps” or other information (info panels, labels and indicators). Unfortunately this method is over the computation/power/space possibilities of today’s embedded systems in mobile devices. It is also possible to equip rooms of a building with a set of transmitters like GPS. But this method is very expensive and complicated. The best method would use the current data infrastructure of the building – the net of mobile Ethernet access points (WiFi, WiMax,...). This

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 755–768, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

method is described in the following paragraphs. A net of access points is not sufficient on its own. For obtaining the right position of mobile devices, it is necessary to equip the device with other sensors and maps. When needed we can dynamically place additional access points to achieve a higher communication range or a higher precision of position detection.

1.1 Need of Orientation and Navigation in Buildings

In our lives, situations can occur when humans need to see more and beyond. Some places are hidden to human vision, are too dangerous or too far away. There is a need to equip the user with some devices which increase human perspective. A special set of mobile devices was built at the Technical University of Ostrava for this purpose. These mobile devices allow the user to get more information about remote places. The first small handheld mobile device is the remote control and provides Human-Machine Interface to the user. The remote control is used for monitoring and controlling the second mobile device – a probe. The two devices are connected using wireless connection.

The probe is equipped with a group of distance, pressure, temperature and other sensors for environment detection. This device is able to move by itself to a desired position. This mobile device can search for people who have been trapped by an earthquake using infra camera and make audio-visual contact before the rescue come. Another example is searching for dangerous chemicals or to find criminals before authorities arrived; this is safer for the control staff. The simplest usage is to send or bring some item to a given position. Remote mobile robots are a common thing now, but this device should fulfill the given task using its own artificial intelligence at the end of the development. In the current phase the mobile robot is able to choose a way to its desired position using preprogrammed scenarios. The current problem is the right navigation in buildings. The set is displayed in (Fig. 1).

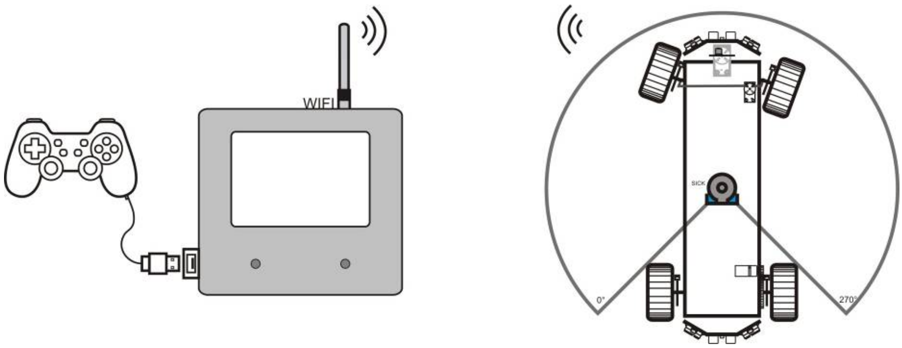


Fig. 1. The set of devices for increased human perspective. On the left side is the remote control with a gamepad in the case of manual mode. On the right side is the probe with sensors and drives. Communication is done by wireless communication.

2 Remote Control

The remote control is the first mobile device from the set. The set should increase human perspective. The remote control provides Human-Machine Interface. The remote control is a medium sized handheld device. It is displayed in (Fig. 2).

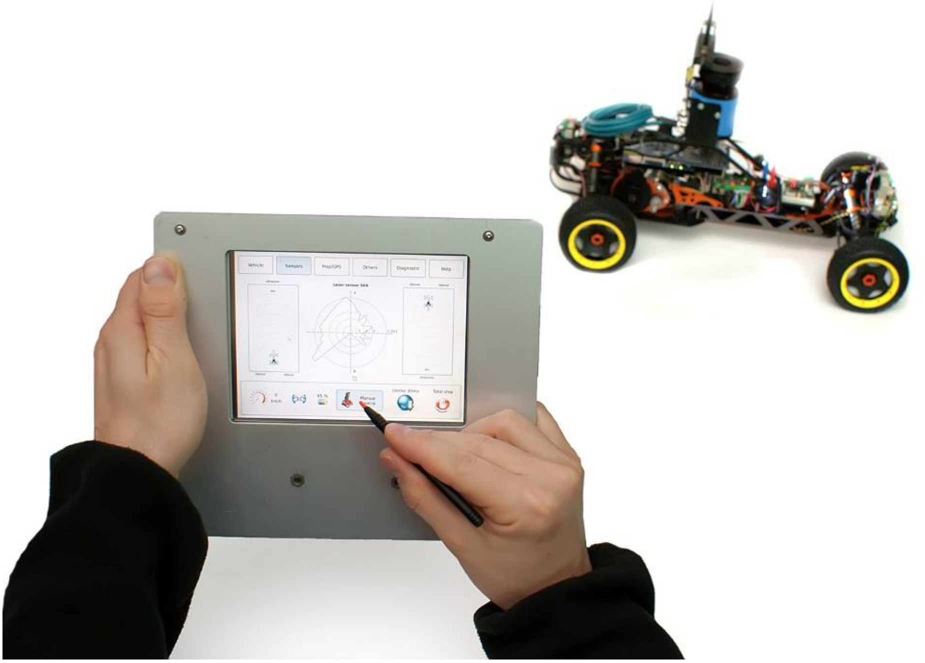


Fig. 2. Human-Machine Interface: Operation panel with color LCD display and touch screen. The controlled probe with sensors and actuator is in the back.

Remote control provides:

- monitor and control of the probe
- display information from sensors
- setting the task or the desired position in auto mode
- manual control using a gamepad or joystick
- maps insertion and actualization
- audio-visual interface
- diagnostic interface with trends and help

The user has full control of the second mobile device (the probe) or he can give the task to the probe. The user can handle the probe using a color display and touch panel. Manual mode is also available. The probe is controlled by a gamepad in manual mode. Programmed application provides intuitive user interface with a set of buttons, value displays and screens. Several screens are displayed in the following pictures. (Fig. 3 to Fig. 6).

First picture (Fig. 3.) displays the situation measured using distance sensors – laser, optical, and pieso. In the situation something is very close to the back of the probe. The only free space to ride is on the right side.

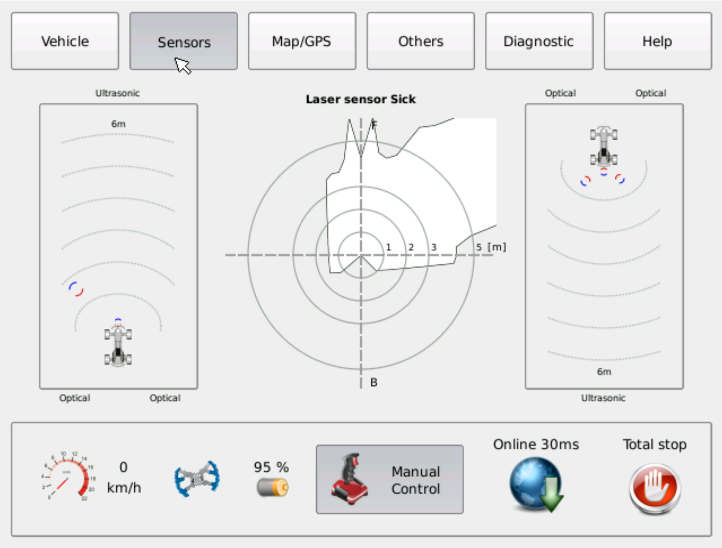
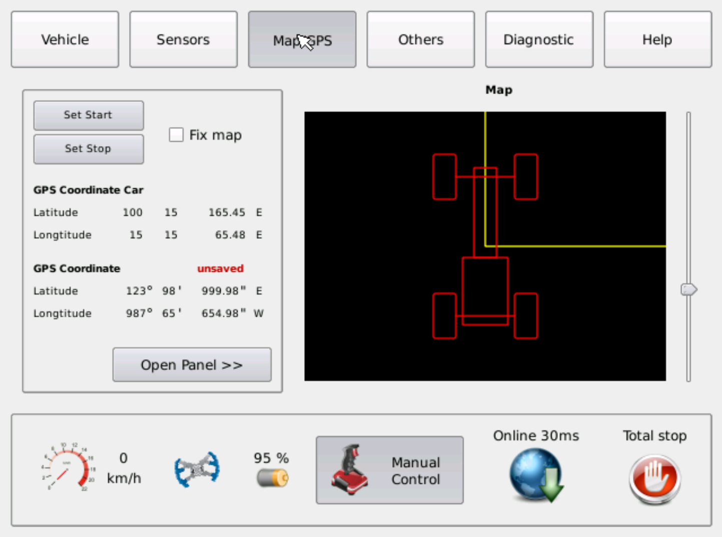
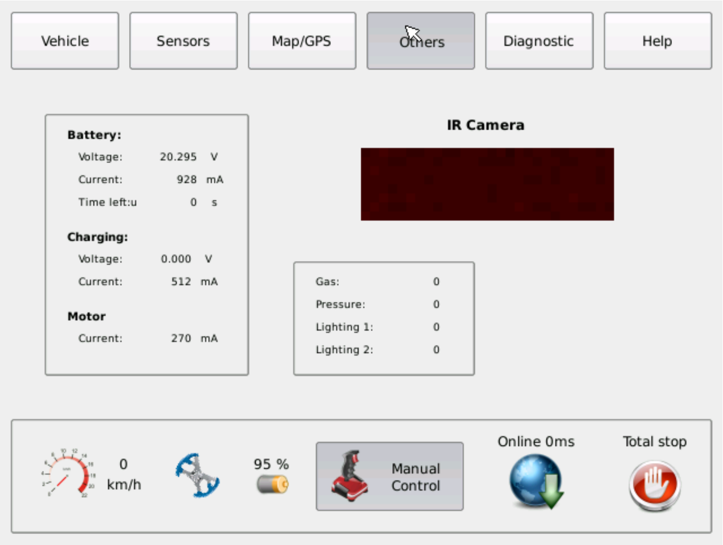


Fig. 3. Sensors screen from remote control application – laser, pieso and infra distance sensors



GPS Coordinate Car				
Latitude	100	15	165.45	E
Longtitude	15	15	65.48	E
GPS Coordinate			unsaved	
Latitude	123°	98'	999.98"	E
Longtitude	987°	65'	654.98"	W

Fig. 4. Position of the probe and maps of remote control application



Battery:
Voltage: 20.295 V
Current: 928 mA
Time left:u 0 s

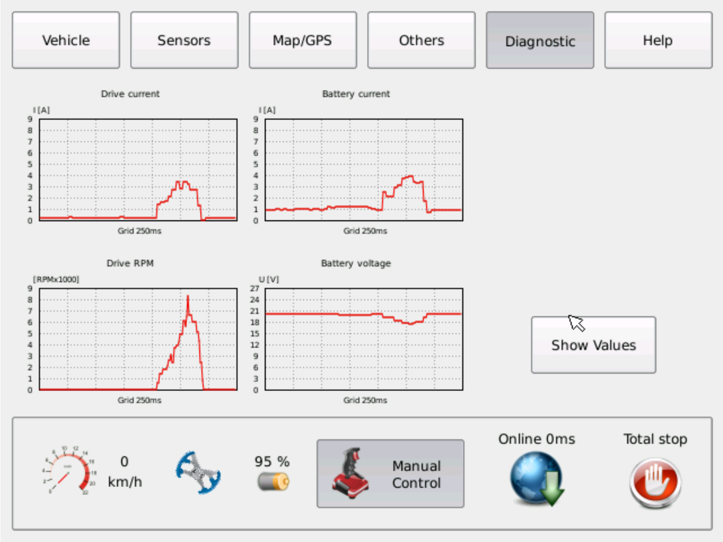
Charging:
Voltage: 0.000 V
Current: 512 mA

Motor
Current: 270 mA

Gas: 0
Pressure: 0
Lighting 1: 0
Lighting 2: 0

0 km/h
95 %

Fig. 5. Camera and diagnostic screen from remote control application



0 km/h
95 %

Fig. 6. Diagnostic screen from remote control application – trends or list of values

Next three pictures (Fig.4 to Fig.6.) illustrate other screens of the remote control.

2.1 Architecture of the Remote Control

The remote control uses the iMX31LiteKit embedded controlling board based on the ARM architecture [13]. The core of the board is the Freescale iMX31 microprocessor.

The embedded board is equipped with a set of interfaces (Ethernet, serial, SPI, SD, CF etc.) The controlling application is stored on external SD card. For debugging purposes, the device is equipped with Ethernet connection. The remote control communicates with the probe using the WiFi module Owspa311 connected via serial interface. The remote control uses a touch panel placed on the color display with a resolution of 640x480 pixels. It is possible to use a gamepad or joystick in the case of manual mode. The architecture is displayed in (Fig. 7).

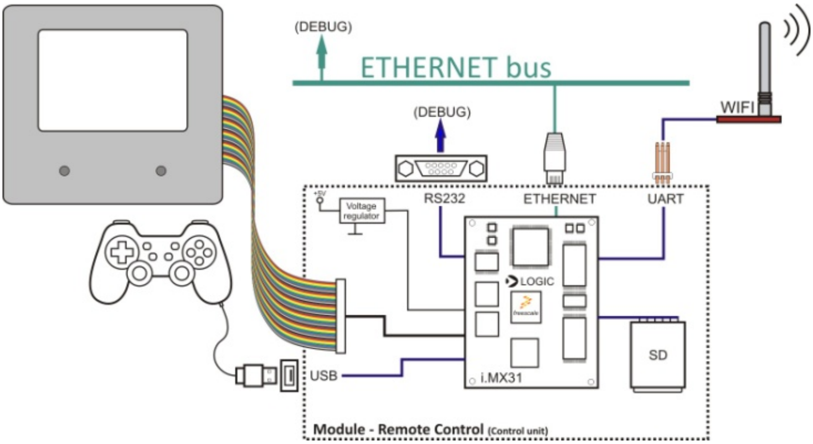


Fig. 7. Architecture of the Remote Control – display, mainboard and WiFi communication

2.2 SW Architecture of the Remote Control

The software application is based on the LinuxLink embedded linux [11]. The application is programmed and compiled using the TimeStorm integrated development environment (IDE) including board support package (BSP) for the iMX31Litekit [12]. The Fedora Linux host machine and the NFS (network file system) are used for developing the application. This way is quite complicated but very fast. The application is compiled and stored on the NFS or on an SD card. After reset (power on) the Logic Loader loads the application from the SD card and starts it.

The application is developed in the Qt graphic tool – Qt Creator. In this tool it is possible to create the design, windows, buttons and main root. To create the final application it is necessary to select an external compiler and to make the application. Another way is to use the Qt designer, which only generates functions and windows. The application is then programmed and compiled in some IDE environment – the TimeStorm in the case of the iMX31.

The QT is a general graphic library which can be used in several operating systems (Windows, X11, Linux). The library is simplified for embedded systems. All necessary servers are already included in the library. The application writes directly to the frame buffer (Fig. 8).

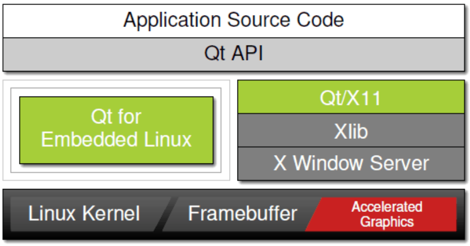


Fig. 8. SW Architecture of control application of the Remote Control

3 Probe

The second mobile device – the probe – is based on a massive chassis with a distributed control system, motor and high capacity battery. It is approximately 85cm meter long and 60cm high without an antenna (Fig. 9). The weight is approximately 10kg including the DC drive, the battery, the CAN based distributed control system and all sensors.

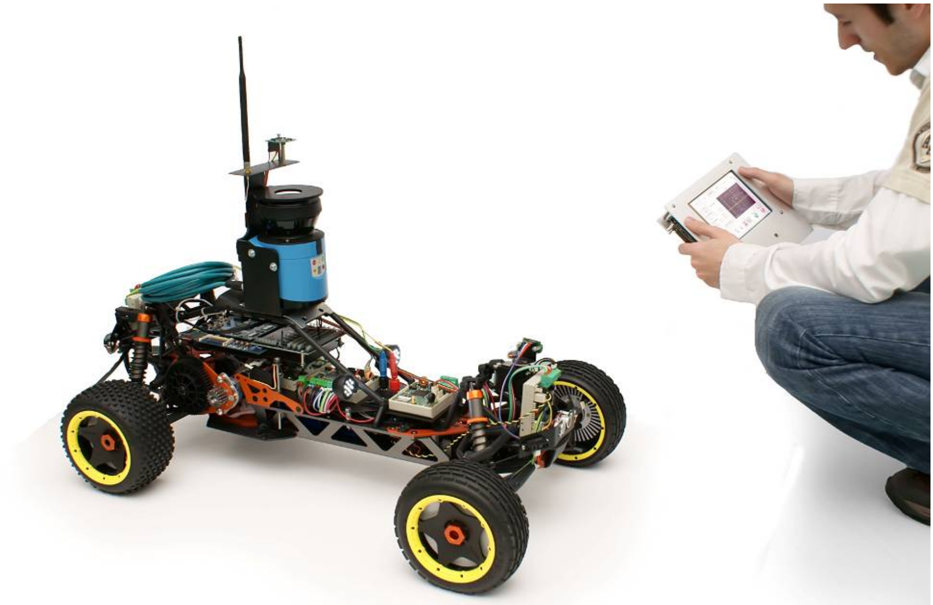


Fig. 9. Probe: Wheeled mobile device equipped with set of sensors

The probe includes a set of sensors for distance measuring, environment measurement and position and movement detection. For example, the Laser scanner can measure an environment up to 20meters in 270 degrees. The probe includes infra-camera, pieso and optical distance sensors, pressure, temperature, GAS sensors, 3-axis accelerometers etc. The audio-visual interface is in the preparation phase.

3.1 Architecture of the Probe

The probe is equipped with a distributed control system with a set of embedded control and monitoring boards. The system is based on the industrial CAN bus and the CANOpen application layer [4] [14].

The main control unit uses the same HW architecture like the remote control. The control unit is based on the iMX31LiteKit and it is also equipped with LinuxLink (Fig. 10).

Other control boards are based on industrial microcontrollers Freescale HCS12 with the cooperation of the FreeRTOS operating system. These boards are programmed using C programming language using the CodeWarrior IDE. The probe communicates with the remote control using the WiFi module Owspa311.

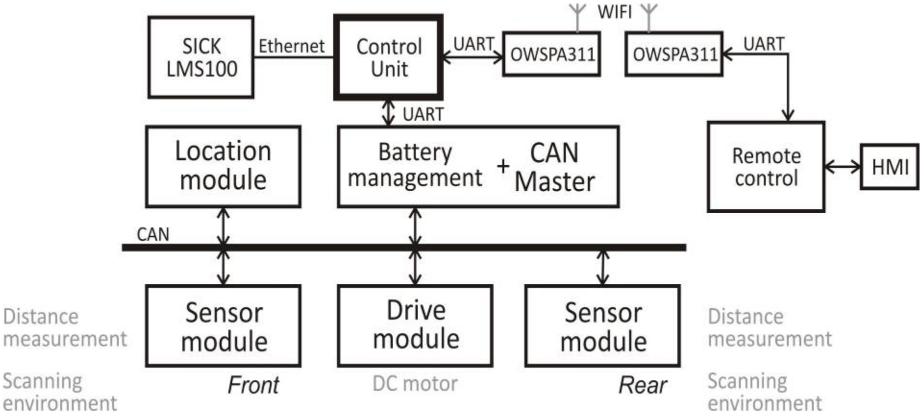


Fig. 10. Architecture of the probe: CAN based distributed control system

3.2 SW Architecture of Main Control Unit of the Probe

The main Control unit of the Probe uses a similar SW platform to the remote control. The software application is based on the LinuxLink embedded linux. The application is programmed and compiled using the TimeStorm IDE environment including BSP for the iMX31Litekit. The Fedora Linux host machine and NFS system is used for developing the application. The application is compiled and stored on the NFS or on the SD card. After starting up, the Logic Loader loads the application from the SD card and starts it (Fig. 11).

The main control application uses several cooperation processes. This method enables the main control system to dynamically start, stop or replace part of the application without influencing the rest of the application.

Used processes:

- vehicle_init – init of the application
- vehicle_guardian – observes run of processes – restarts if not responding
- vehicle_memory – data block – all values of the probe

- vehicle_slave – communicates with slave units and writes data to the shared memory
- vehicle_wifi – communicates with the remote control
- sick – reads data from sick laser scanner –writes data directly to the shared memory
- vehicle_control – main control, finds the path, maps.

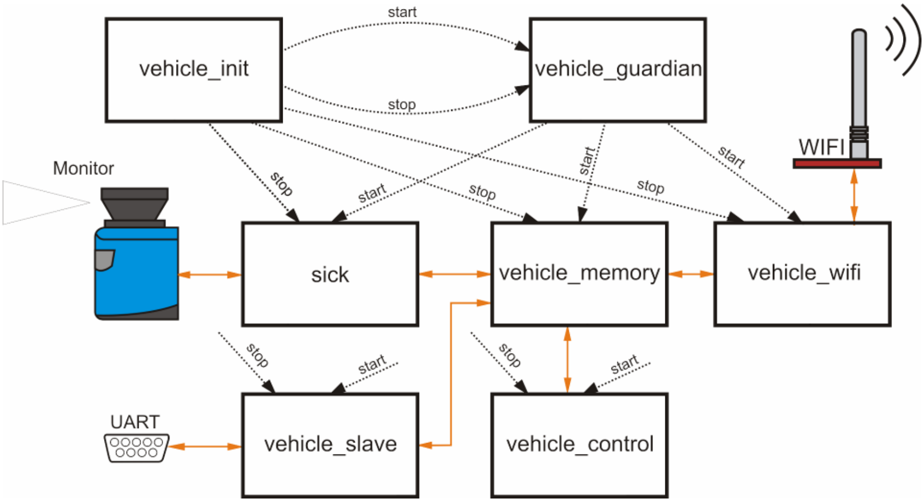


Fig. 11. Architecture of the probe: CAN based distributed control system

4 Localization

Another important part of the project is based on indoor localization. The primary localization is needed to detect a position inside the building. Consequently, the map of the detected location is loaded into a mobile device to activate other sensors to "open the eyes" of our mobile devices. The localization is made through a WiFi infrastructure.

If the mobile device knows the position of the stationary device (transmitter), it also knowsits own position within a range of this location provider. The typical range varies from 30 to 100 m where there is WiFi, respectively 50 m where there is BT case or 30 km for GSM. Granularity of the location can be improved by triangulation of two or more visible APs (Access Points). The mobile client currently supports the application in automatically retrieving location information from nearby WiFi, BT and GSM location providers, and in interacting with the PDPT server. The application (locator) is implemented in C# language using the MS Visual Studio .NET with .NET Compact Framework and a special OpenNETCF library enhancement.

A first key step of the localization is a data collection phase. The information about the radio signals is recorded as a function of a user's location. The signal information is used to construct and validate models for signal propagation. Among other information, the signal strength (SS) is available where WiFi, BT and GSM networks are available.

To get a user position with more accuracy, the triangulation is currently used in PDPT framework. Other localization techniques like Monte Carlo localization can be used to get a better position if it is needed, but the PDPT framework provides good results only with triangulation techniques on a basic level of localization.

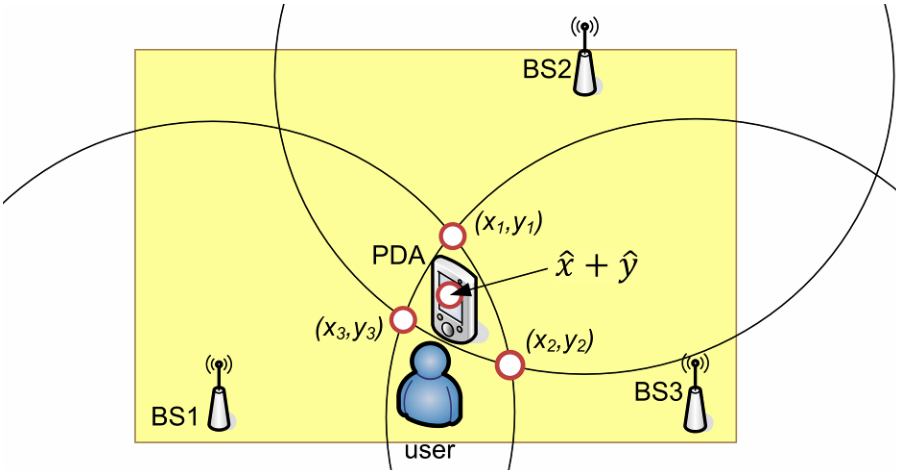


Fig. 12. Localization principle – trilateration

In a testing model (Fig. 12) the mobile client gets the SS info of three BSs (Base Stations) with some inaccuracy. Inaccuracy is caused by SS value from a mobile device wireless module, where only SS in present. Circles around the BSs (in real 3D space the sphere is used around the BSs representing SS value) are crossed in red points in the figure. The red point intersection (centre of three) is the best computed location of the mobile user. The user track is also computed from these locations and it is stored in a database for later use. This idea is applicable in the case of WiFi as well as BT and GSM networks.

4.1 WiFi Localization

In a real case of indoor localization by WiFi networks, several types of environments are used like open spaces, walls and mixed spaces. The Cisco APs (Cisco Aironet 1121 and 1131) are used in the test environment at the Technical University of Ostrava.

The measurements on three selected (representing three types of environment) APs of all APs have been performed to get signal strength (SS) characteristics. The characteristics were combined to get a one characteristic called "Super-Ideal characteristic". The computed equation for Super-Ideal characteristic is taken as basic equation for PDPT Core to compute the real distance from WiFi SS. The equation has a sufficient coefficient of determination $R^2 = 80\ \%$ (R^2= ssreg/sstotal).

In the case of in-door location the damping effect of walls especially when the number of BS´s is small could hamper the positioning. However the precise positioning is not needed in all cases. When the granularity of object areas to be prebuffered into the mobile device cache is in level less than tens of meters, the localization by one or two visible BS´s is possible with high level of success. Maximal location error for static localization is 25 meters for the case the only 1 WiFi AP is in the range, 7 meters for 2 APs in range, resp. less than 5 meters in case of 3 or more WiFi APs (mentioned Cisco models) in range. This localization error can be rapidly reduced by use of dynamic localization in a sense of user movement trajectory computation. Naturally, this localization principle can be applied to other wireless technologies like Bluetooth, GSM or WiMAX.

5 The PDPT Framework

The PDPT framework server is developed as a web service to act as a bridge between SQL Server (contain WLA database) and PDPT Clients (Fig. 13). Client mobile application contains a location sensor component to scan nearby for WiFi APs. WiFi SS info is continuously transferred to the PDPT Framework Core. This component computes the user's location information from WiFi SS. In next step the PDPT Core makes a decision to which part of WLA Server database needs to be replicated to client's SQL Server CE database [9][10]. The PDPT Core decisions constitute the most important part of PDPT framework, because the kernel must continually compute the position of the user and track, and predict his future movement. After doing this prediction the appropriate data are prebuffered to client's database for the future possible requirements. This data represent artifacts list of client buffer imaginary image.

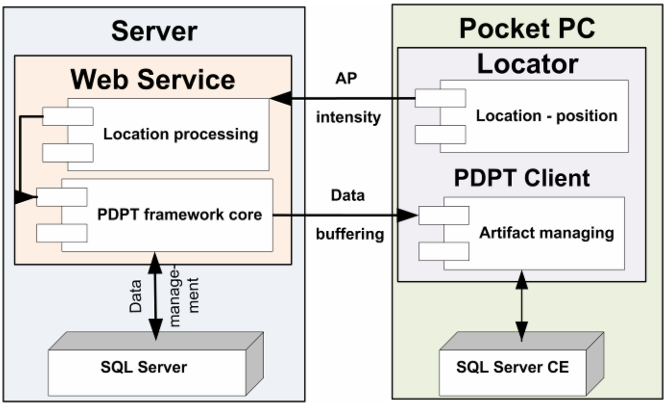


Fig. 13. PDPT architecture – UML design

5.1 Data Artifact Creating

Artifact represent an object in WLA SQL server database with image, audio, video or other file types. Every artifact must have associated with position coordinates in 3D environment (S-JTSK format is used). Open source software Quantum GIS is used to manage all data in 3D spaces like building map basis, APs location and artifacts location. To manage and work with locations of artifacts, firstly the building floor map is needed to obtain. In most cases the scanned version is adequate. The obtained map needs to be converted to Tagged Image File Format (TIFF). Location coordinates for such file must be created in TFW separate file. TFW file contains coordinates that describe the location, scale, and rotation of a map formatted as a raster TIFF image. All obtained position info must be stored in PDPT Core web service. Artifacts with position coordinates are stored in WLA database by "WLA Database Artifact Manager".

5.2 Data Artifact Managing

The WLA server database manages the artifacts in the context of their location in building environment. The PDPT Core selecting the data to be copied from PDPT server to mobile client by context information (position info). Each database artifacts must be saved in database with the information about area to which it is belong.

A software application called "Data Artifacts Manager" was created to manage the artifacts in WLA database. User can set the priority, location, and other metadata of the artifact. The Manager allows creating a new artifact from multimedia file source (image, video, audio, etc.), and work with existing artifacts [9].

5.3 PDPT Core - Area Definition for Selecting Artifacts to Buffering

The PDPT buffering and predictive PDPT buffering principle consists of several following steps. Firstly the client must activate the PDPT on PDPT Client. This client creates a list of artifacts (Client buffer image), which are contained in his mobile SQL Server CE database. Server create own list of artifacts (imaginary image of Client buffer) based on area definition for actual user position and compare it with real Client buffer image. The area is defined as an object where the user position is in the center of object. The cuboid form is used in present time for initial PDPT buffering. This cuboid has a predefined area with a size of 10 x 10 x 3 (high) meters. The PDPT Core continues in next step with comparing of both images. In case of some difference, the rest artifacts are prebuffered to Client buffer. When all artifacts for current user position are in Client buffer, there is no difference between images. In such case the PDPT Core is going to make a predicted user position. On base of this new predicted user position it makes a new predictive enlarged imaginary image of Client buffer. The size of this new cuboid is predefined area of size 20 x 20 x 6 meters. The new cuboid has a center in direction of predicted user moving and includes a cuboid area for current user position. The PDPT Core compares the both new images (imaginary and real Client buffer) and it will continue with buffering of rest artifacts until they are same. Creation of an algorithm for dynamic area definition is better in real case of usage to adapt a system to user needs more flexible in real time [10].

6 Terain Identification and Navigation

The problem of orientating and navigating mobile devices in building divides into three options. The first option is orientation in a known place. It is assumed that the device is equipped with the map of the place. The only problem is to get the current position in relation with the map. The second option is the dynamic download of the necessary part of the map based on the current position – for example, the PDPT Framework. The third option is an unknown place. So the mobile system has to be able to dynamically recognize the environment and to dynamically generate the map. Then the mobile device has to find the way using some method.

The probe computes the current position based on four parts of information:

1. The probe approximates the position based on the WiFi connection or gets the position from GPS.
2. Map of the environment (stored or dynamically downloaded).
3. Clarifies the position in the map using sensors and possible positions.
4. Relative change of the position based on incremental sensors and accelerometers.

When the probe knows its current position it can reach the target position.

1. Using the map and Dijkstra's algorithm it will obtain the shortest path tree.
2. The probe first gets an item from the list – the current position to the first intersection.
3. Reach the intersection using the drive.
4. Check obstacles on the road.
5. Gets next branch from first intersection to second one.
6. If there is an obstacle turn left or right with 60 degrees based on space on sides of the road (sensor system).
7. Go back to previous direction – second intersection.
8. Repeat until target position is reached.

During the ride it is necessary to check the state of the embedded power source – the battery. Power consumption of the probe is displayed in (Fig. 14). During the ride the average power consumption of the probe is approximately 2.3 Ampers. The capacity of the battery is 4.6 Ah. So the probe can work in an active state for a maximum of 2 hours.

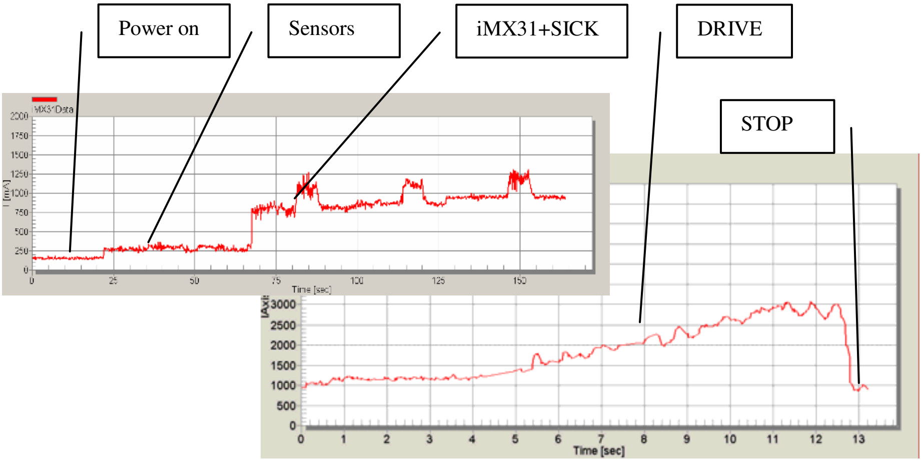


Fig. 14. Power consumption of the probe in five different states

The solar panel is prepared for charging the battery during the ride for the future. In the case of low energy the probe will stop, turn off the sensor system and wait to charge the battery.

7 Conclusion

The main aim of the project is to give the tool to the user which can extends the user perspective. The current state of the project is testing the set of mobile devices at the Technical University of Ostrava. The WiFi network is used for orientation in cooperation with local maps. The mobile device is equipped with an algorithm for finding the best way from the current to desired position. In the future the PDPT algorithm and dynamic generation of the map based on information from sensors will be implemented.

References

1. Abowd, G., Dey, A., Brown, P., et al.: Towards a better understanding of context and context-awareness. In: Gellersen, H.-W. (ed.) HUC 1999. LNCS, vol. 1707, p. 304. Springer, Heidelberg (1999)
2. Krejcar, O.: User Localization for Intelligent Crisis Management. In: AIAI 2006, 3rd IFIP Conference on Artificial Intelligence Applications and Innovation, pp. 221-227 (2006)
3. Krejcar, O., Cernohorsky, J.: Database Prebuffering as a Way to Create a Mobile Control and Information System with Better Response Time. In: Bubak, M., van Albada, G.D., Dongarra, J., Sloot, P.M.A. (eds.) ICCS 2008, Part I. LNCS, vol. 5101, pp. 489–498. Springer, Heidelberg (2008)
4. Kotzian, J., Srovnal, V.: Distributed embedded system for ultralight airplane monitoring. In: sborníku (ed.) ICINCO 2007, Anger, France, vol. 2007/1, pp. 448–451 (2007), ISBN 978-972-8865-82-5
5. Kotzian, J., Srovnal, V.: Can Based Distributed Control System Modelling Using UML. In: Proceeding International Conference IEEE ICIT 2003, Maribor, Slovenia, pp. 1012–1017 (2003), ISBN 0-7803-7853-9
6. Nielsen, J.: Usability Engineering. Morgan Kaufmann, San Francisco (1994)
7. Haklay, M., Zafiri, A.: Usability engineering for GIS: learning from a screenshot. The Cartographic Journal 45(2), 87–97 (2008)
8. Evennou, F., Marx, F.: Advanced integration of WiFi and inertial navigation systems for indoor mobile positioning. Eurasip journal on applied signal processing (2006)
9. Krejcar, O.: Full Scale Software Support on Mobile Lightweight Devices by Utilization of all Types of Wireless Technologies. In: Granelli, F., Skianis, C., Chatzimisios, P., Xiao, Y., Redana, S. (eds.) Mobilight 2009. LNICST, vol. 13, pp. 173–184. Springer, Heidelberg (2009)
10. Krejcar, O.: Problem Solving of Low Data Throughput on Mobile Devices by Artefacts Prebuffering. EURASIP Journal on Wireless Communications and Networking, Article ID 802523, 8 pages (2010)
11. Timesys (online) (2010), LinuxLink, `https://linuxlink.timesys.com/3/Products` (cit. 2010-03-17)
12. Timesys (online) (2010), TimeStorm `https://linuxlink.timesys.com/3/Products/TimeStorm` (cit. 2010-03-17)
13. Zoom (online) (2010), Frescale Zoom i.MX31 LITEKIT, `http://www.logicpd.com/products/development-kits/freescale-zoom%E2%84%A2-imx31-litekit` (cit. 2010-03-17)
14. CiA (online), CAN in Automation (2010), `http://www.can-cia.org/` (cit. 2010-03-17)

Architecture and Design of Mobile Telemetry System for Ambient Assisted Living

Martin Stankus[1], Marek Penhaker, Jan Kijonka,
Petr Grygarek, and Jiri Kotzian

VSB - Technical University of Ostrava, Faculty of Electrical Engineering and Computer Science,
17. listopadu 15, Ostrava, Czech Republic
{martin.stankus,marek.penhaker,jan.kijonka,
petr.grygarek,jiri.kotzian}@vsb.cz

Abstract. Mobile systems for ambient assisted living are of growing importance in present world. This article describes architecture and design of such system including it's logical partitioning into functional blocks and placement of these blocks. Although full description of discussed system is beyond scope of this paper, description of processed biomedical and other data is provided as well as implementation details including types of used parts, cooperation of these parts, intraction of system with user and used communication protocol.

Keywords: biotelemetry, measurement, microcontroller, ZigBee.

1 Introduction

Monitoring of vital functions is usually performed only in specialized medical facilities equipped with costly equipment. But it's desirable to perform monitoring of vital functions in user's home environment as well. As monitoring in home environment is performed without direct participation of medial staff, whole system has to be of autonomous nature. It's expected that home monitoring system is deployed for prolonged periods od time. Because of this, interference of system with standard behavior of user should be as small as possible. Whole system must be reliable as user's life may depend on monitoring of vital functions. Purpose of this article is to describe architecture of such system.

2 Architecture of System

Architecture of system for remote monitoring of vital functions can be partitioned into two partially independant functional blocks. First (inner) block is composed of devices located in space where user spends most of his time. Primary purpose of inner block is measurement of biometric and other values as well as forwarding of these data. Second (outer) block is composed of devices located in supervision centre. Outer block is common for multiple instances of inner block. It's primary purpose is evaluation and archivation of values measured in instances of inner block.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 769–780, 2010.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010

2.1 Inner Block of Architecture

Entire instance of inner block is located in space where user spends most of his time. It's purpose is measurement of various values and forwarding of these values to outer block. Because of diverse nature of measured values, it's necessary to further partition inner block into functional elements. This partitioning can be seen in Fig. 1.

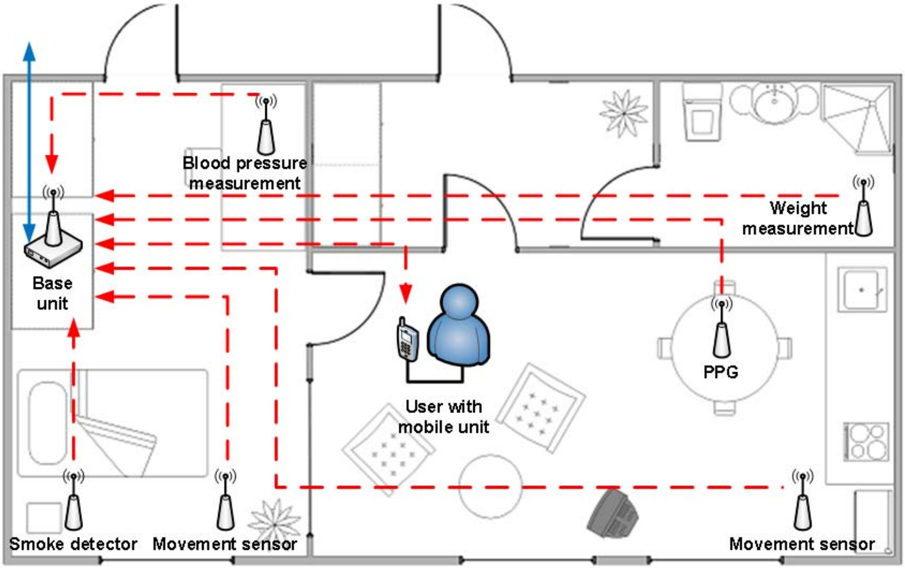


Fig. 1. Inner block of architecture

As can be seen in Fig. 1, measurements are performed by two classes of devices - by mobile unit, which is always in close proximity to user and by specialized stationary sensors. Some of measured biometric values, for example ECG, require continuous attachment of sensors to user's body. Other measured values should be measured periodically, for example temperature. These requirements can be fulfilled if user is equipped with mobile unit of suitable design. Another kinds of measures should be performed by stationary measurement devices, examples of these are measurements of blood pressure by sphygmomanometer. Values measured inside of inner block are transmitted to stationary base unit. It's task of this unit to transport these data outside of inner block or cache them temporarily in case of uplink connection failure. Wireless communication inside of inner block is marked red in Fig. 1, communication between inner and outer block is marked blue.

2.2 Measured Values

Home care platform allows monitoring of many values. Some of these values are not of biomedicinal kind. Measured values can be divided by their semantics and periodicity of measurement. Semantically are measured values divided to values of biometric kind and other values. By periodicity of measurement are measured values divided to values measured synchronously and values measure asynchronously. List of measured values can be seen in Tab. 1.

Table 1. Measured values

Measured values	**Sync. measurements**	**Async. measurements**
Biometric values	Two channel ECG	Blood oxygen saturation
	Body temperature	Pulse frequency
	Change of user's position	Blood pressure
		Body weight
Non-biometric values	Ambient temperature	Person occurance in room
	Change of mobile unit's position	Smoke occurance in room

Measures are performed by two classes of devices - by multipurpose mobile unit performing synchronous measurements and by dedicated sensors performing asynchronous measurements. Division of measured values by type of measuring device can be seen in Tab. 2.

Table 2. Division of measured values

Generating device	**Type of measurement**
Mobile unit	Two channel ECG
Mobile unit	Body temperature
Mobile unit	Change of user's position
Stationary sensor - PPG	Blood oxygen saturation
Stationary sensor - PPG / blood pressure meas.	Pulse frequency
Stationary sensor - blood pressure meas.	Blood pressure
Stationary sensor - weight measurement	Body weight
Mobile unit	Ambient temperature
Mobile unit	Change of mobile unit's position
Stationary sensor - movement sensor	Person occurance in room
Stationary sensor - smoke detector	Smoke occurance in room

Biometric sychronously measured values are two channel electrocardiograph (ECG), body temperature and changes in user's position. Some values of non-biometric type are measured synchronously as well. Examples of these are ambient temperature and changes in position of mobile unit. By measuring changes in position of both user and mobile unit, it's possible to detect fall of user or drop of mobile unit. Asychronous measures requiring user's direct participation are measurements of blood oxygen saturation, pulse freqency, blood pressure and body weight. Asynchronously measured values of non-biomedical type are monitoring of smoke occurance and presence of persons in user's flat. These measurements are rather of security character. Every measured character is specific and has associated it's own data type. Synchronously measured values are sampled with specific sampling frequency. List of these parameters can be seen in Tab. 3 and Tab. 4.

Table 3. Parameters of measured values

Type of measurement	**Range of data sample**	**Range of meas. val.**
Two channel ECG	12 bits,4096 values (for each chan.)	0.1000 - 10.0000 mV
Body temperature	8 bits,256 values	30.0000 - 45.9375 C
Change of user's position	10 bits,1024 values (for each axis)	-3.0000 - 3.0000 g
Blood oxygen saturation	8 bits,256 values	0 - 100 %
Pulse frequency	8 bits,256 values	0 - 255 pulses/s
Blood pressure	8 bits,256 values (sep. syst./diast.)	0 - 255 mm/Hg
Body weight	16 bits,65636 values	0.0000 - 4095.9375 Kg
Ambient temperature	8 bits,256 values	-64.0 - 63.5 C
Change of mob. unit's pos.	10 bits,1024 values (for each axis)	-3.0000 - 3.0000 g
Person occurance in room	1 bit,2 values	yes - no
Smoke occurance in room	1 bit,2 values	yes - no

Table 4. Parameters of measured values (cont.)

Type of measurement	**Granularity of meas.**	**Meas. per 1 sec**
Two channel ECG	0.0024 mV	300
Body temperature	0.0625 C	1/120
Change of user's position	0.0059 g	125
Blood oxygen saturation	1 %	—
Pulse frequency	1 pulse/s	—
Blood pressure	1 mm/Hg	—
Body weight	0.0625 Kg	—
Ambient temperature	0.5 C	1/120
Change of mob. unit's pos.	0.0059 g	125
Person occurance in room	—	—
Smoke occurance in room	—	—

2.3 Communication in Inner Part of Architecture

Basic building block of communication inside of inner part of architecture is ZigBee wireless technology. ZigBee is specialized communication technology optimized for industrial and medicinal deployment. Raw bandwidth of ZigBee network is 250 kbps. Real throughput of ZigBee network is somewhat lower but is still more than sufficient for data transmission in home care system. Individual instances of inner block are identified by locally unique ZigBee Personal Area Nework Identification (PAN ID) number. This way it's possible to operate multiple instances if inner block and their respective ZigBee networks in close vicinity. Communication is encrypted by 128-bit Advanced Encryption Standard (AES) cipher. Scheme of communication can be seen in Fig. 2.

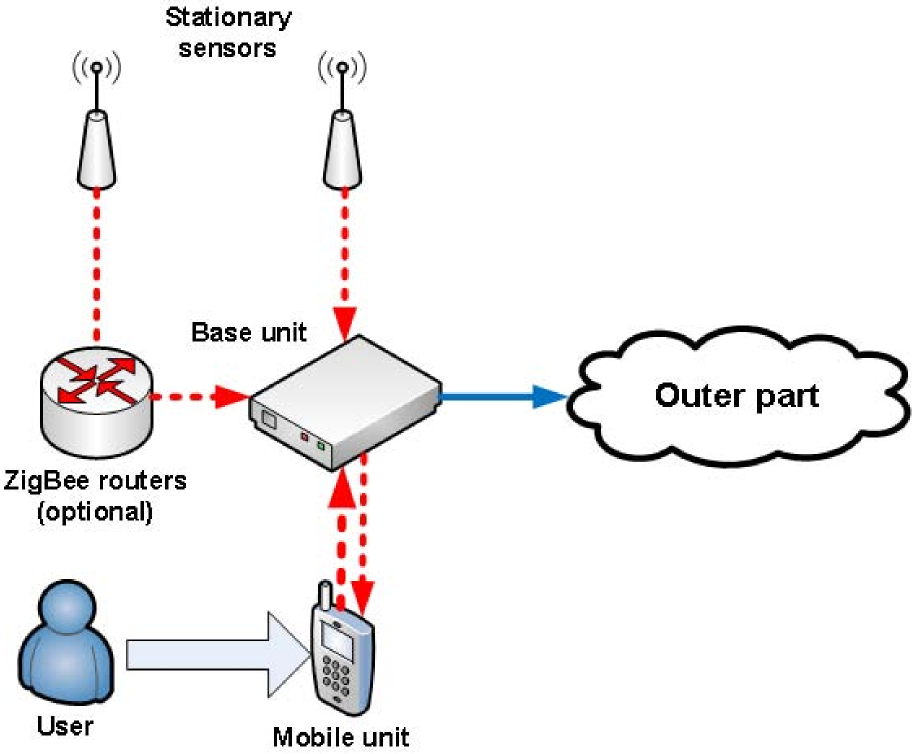


Fig. 2. Communication in inner part of architecture

Every flow of measured data is identified by logical address in ZigBee network. This is address of ZigBee cluster. ZigBee cluster is logical data channel transporting individual types of measured data. Data generated by class of stationary sensors are forwarded to mobile unit by base station. This way, user can be presented with full scale of his own measured values.

3 Construction of Inner Part of Architecture

Central part of mobile unit is power efficient 32-bit reduced instruction set computer (RISC) microcontroller (MCU) of ARM7TDMI microarchitecture. Clock frequency of microcontroller is set at 48 MHz. With this clock frequency, microcontroller provides computational performance of approximately 43 million instructions per second (MIPS). ZigBee network is implemented using dedicated ZigBee chipset offloading ZigBee networking tasks. Measured data are temporarily stored in fast nonvolatile FRAM memory in case of ZigBee network failure. Mobile unit itself resembles mobile phone with LCD display and keyboard allowing interaction with user. Controller of LCD display and keyboard is implemented using simple 8-bit MCU. Peripheries are connected to central 32-bit MCU by SPI (4 Mbps) and I2C (100 kbps) serial busses.

4 Interaction with User

Low power CMOS 8-bit MCU based on Atmel AVR core is used as user interface controller. Main function of user interface MCU is to receive respective measured values from central ARM MCU and provide user with them. User can interact with mobile unit using simple pushbutton keyboard. Clock frequency of MCU is set to 12 MHz, maximal frequency for used 3.3 V power rail voltage. Current requirement is about 7 mA in active mode and 0.2 A in stand-by mode. User interface MCU allows for communication with other components of user interface, namely LCD, keyboard, external data flash memory and external components like central ARM MCU. Block diagram of entire mobile unit can be seen in Fig. 3.

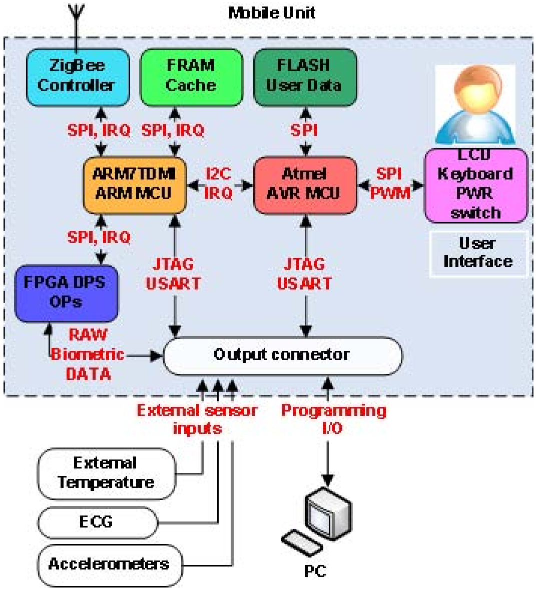


Fig. 3. Block scheme of mobile unit

4.1 User Data Flash Memory

Flash memory with SPI interface is used as external data flash memory. Its 8 Mb of space is organized as 4096 pages of 256 or 264 bytes each. Flash memory allows for intelligent memory operations like selective page programming and flexible erase operations (page, block, sector, chip erase). 100 000 program/erase cycles per page are guaranteed.

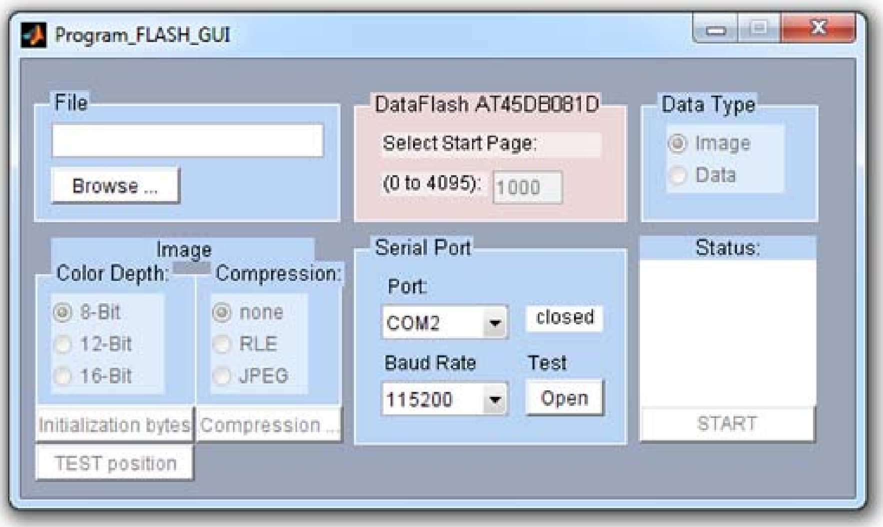
User data flash memory contains following data:

- Image data (icons, user menu panels, battery and signal strength states, map of monitored area) are stored in uncompressed RGB format suitable for direct LCD operations.

- Fonts (3 font styles 6x8, 8x8 and 8x16 pixels).
- Trend data (temperatures, blood pressure, blood oxygen saturation, body weight and others).
- Various settings.

4.2 Content of Data Flash Memory

Application designed in Mathworks Matlab is used for manipulation of user data flash memory. Connection between mobile unit and workstation is achieved by RS232 interface. Graphical user interface of application can be seen in Fig. 4.



DataFlash AT45DB081D
Select Start Page:
(0 to 4095): 1000

Data Type: ● Image ○ Data

Image Color Depth: ● 8-Bit ○ 12-Bit ○ 16-Bit

Compression: ● none ○ RLE ○ JPEG

Serial Port
Port: COM2 closed
Baud Rate: 115200

Fig. 4. Data flash management application

Images have to be stored in flash memory in format suitable for displaying on LCD screen. Used PCF8833 LCD controller supports 3 data formats; 8-bit, 12-bit or 16-bit colors. Uploaded images have to be corresponding format.

4.3 LCD Interfacing

LCD is controlled by Philips PCF8833 driver. PCF8833 is single chip low power CMOS LCD controller, designed to drive color Super-Twisted Nematic (STN) displays of 132 rows and 132 RGB columns. All necessary functionality for LCD operation is provided in single chip, including 209 kbit (132 x 12-bit x 132) of RAM. PCF8833 is connected by 3-wire serial interface. PCF8833 has 2 types of accesses. Access for definition of operating mode of the device (instruction) and access for actual RAM operations (data). Efficient data transfer is achieved by autoincrementing of RAM address pointers. The LCD has simple serial interface using 9-bit long words with clock speed of 6.6 MHz. LCD has LED backlight powered by 7 V power source. Its necessary to use the DC-DC step-up converter for LED backlight power supply. Suitable step-up converter is MC34063 switching regulator. Backlight intensity is regulated by PWM signal generator embedded in MCU.

4.4 LCD User Interface

User can display waveforms of vital functions and additional data. User also has option of executing an emergency call. Display is partitioned into several areas. Each of these areas is of specific purpose as can be seen in Fig. 5. Visualisation of various trenda data can be displayed by selection of appropriate menu item. Examples of these visualisations can be seen in Fig. 6, Fig. 7 and Fig. 8.

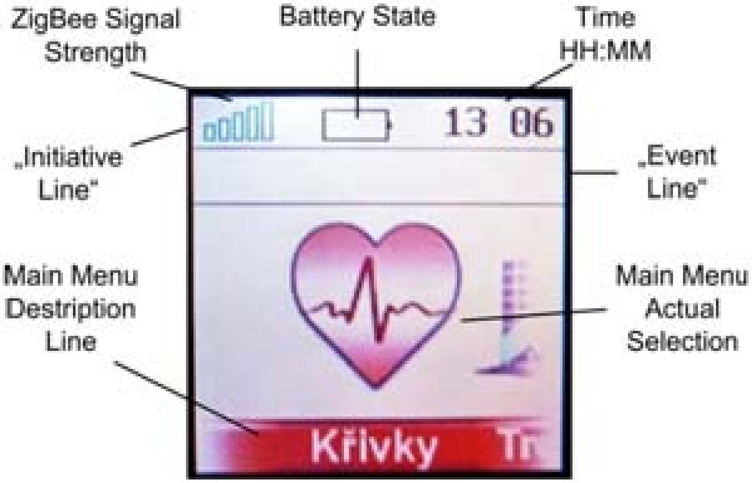


Fig. 5. Top menu area

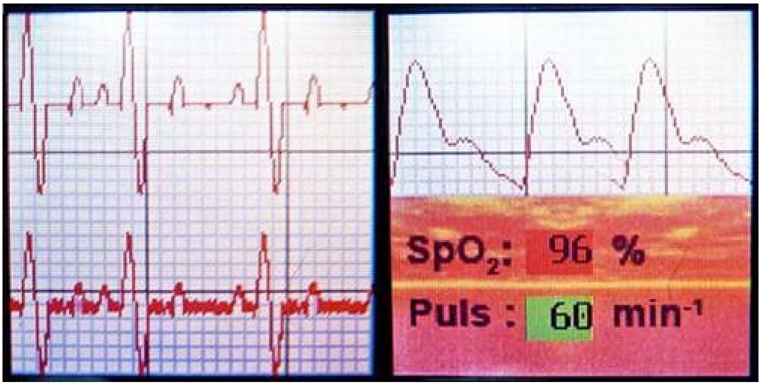


Fig. 6. Two channel ECG and PPG

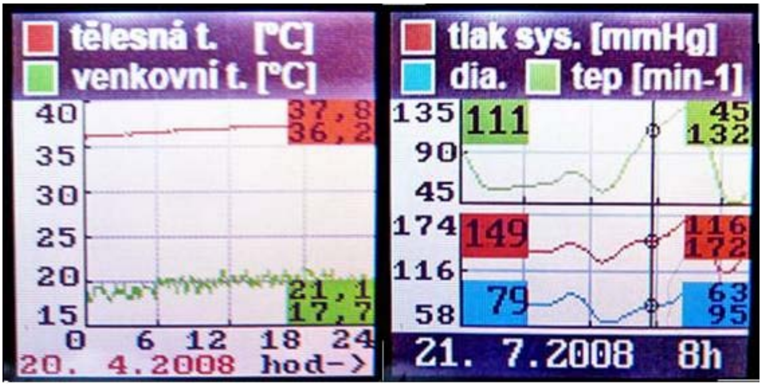


Fig. 7. Body and ambient temperatures, blood pressure

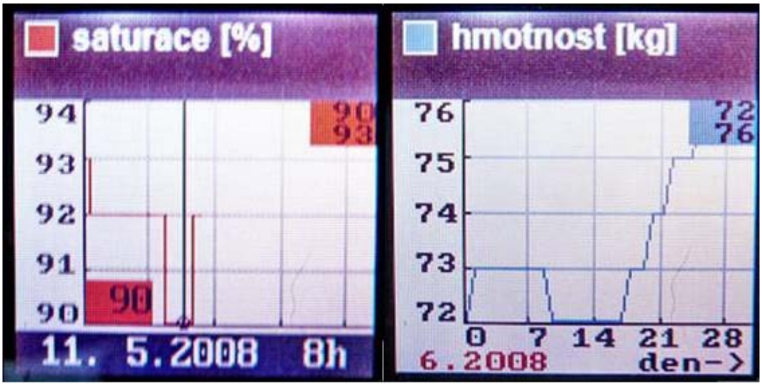


Fig. 8. Blood oxygen saturation and body weight

5 Outer Part of Architecture

Demarcation points between particular instances of inner block and outer block are base units. Fundamental task of entire outer block is to evaluate and archive data measured in instances of inner block. This functionality is implemented by supervision centre as can be seen in Fig. 9.

Measured values are archived by supervision centre in database of measure values. Each instance of inner block performing monitoring of one user is identified by locally unique PAN ID. This PAN ID serves as primary key identifying data of particular user in database. Supervision centre has set of ranges defined for every user. These ranges determine desirable values for each measured data type. Operator of supervision centre informed in case of exceeding of given range. Another element in outer part of architecture is management server. Purpose of management server is to provide auxiliary functionality necessary for

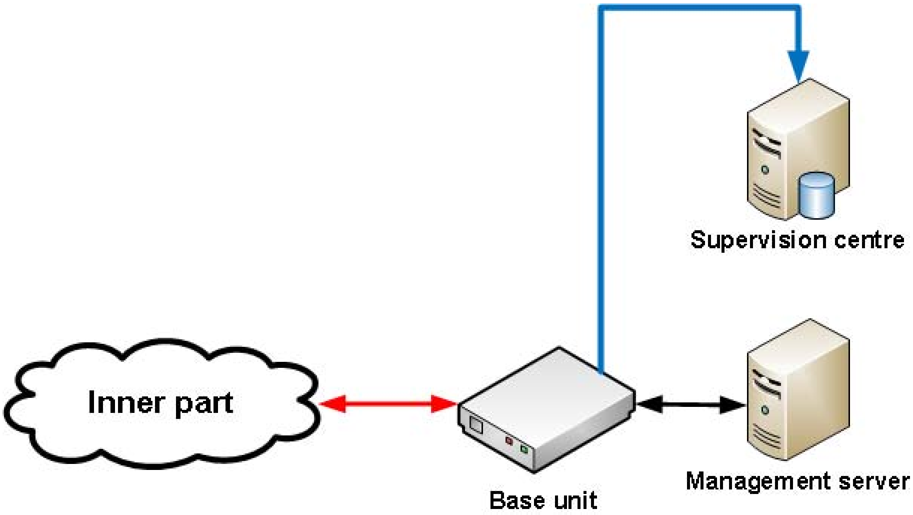


Fig. 9. Outer part of architecture

operation of instances of inner block. Some of the more important examples of this functionality are IP address assignment and remote management.

5.1 Construction of Outer Part of Architecture

Communication in outer part of architecture is at physical and data link layer of network stack implemented by Ethernet technology. Selection of transport media (metallic or optical solution) depends on required distance between given instance of inner block and outer block. It's possible to use suitable WAN technology for tunneling of Ethernet frames in case of greater distance, for example xDSL or DOCSIS. Bandwidth of today's implementations of Ethernet technology is more than suitable for transport of biomedial data. Maximal amount of data genereted by each instance of inner block is limited by bandwidth of ZigBee network to 250 kbps of raw data. It's possible to transport data from thousands instances of inner block if link connecting supervision centre is implemented with 1000 Mbps Ethernet network. Communication is implemented using TCP/IP protocol at network and transport layers. Connection-oriented TCP protocol ensures reliable transport of measured data. Address of ZigBee cluster is used as unambiguous identification of measured data type transported in particular TCP connection. Connectionless UDP protocol is used for implemetation of auxiliary funcionality. Examples of this funcionality is provisioning of instances of inner block, specifically assignment of IP addresses and remote management by SNMP protocol.

6 Conclusions

Described architecture and design of mobile telemetry system for ambient assisted living is result of rigorous testing and evaluation of real solutions. Nevertheless, there is always space for improvements of such system. Described system is primarily aimed at indoor use. Future revisions of system will be designed as outdoor operable including 3G mobile data connection. As mobile unit is battery powered, future development will be aimed at further reduction of power consumption.

Acknowledgment

The work and the contribution were supported by the project Grant Agency of Czech Republic GACR 102/08/1429 "Safety and security of networked embedded system applications". This work was supported by the Ministry of Education of the Czech Republic under Project 1M0567. This work was partially supported by the faculty internal project,"Biomedical engineering systems V".

References

1. Demus, D., Godby, J., Gray, G.W., Spiess, V., Vill, V.: Handbook of LiquidCrystals. Willey, VCH (1998)
2. Farahani, S.: ZigBee Wireless Networks and Transceivers, Newnes (2008)
3. Penhaker, M., Cerny, M., Martinak, L., et al.: HomeCare, Smart embedded biotelemetry system. In: IFMBE proceedings World Congress on Medical Physics and Biomedical Engineering, Seoul, South Korea, August 27-September 01, vol. 14, pp. 711–714 (2007), ISSN: 1680-0737, ISBN: 978-3-540-36839-7
4. Penhaker, M., Cerny, M.: The Circadian Cycle Monitoring. In: Conference Information: 5th International Summer School and Symposium on Medical Devices and Biosensors, Hong Kong, Peoples R China, June 01-03, pp. 41–43 (2008), ISBN: 978-1-4244-2252-4
5. Penhaker, M., Cerny, M., Rosulek, M.: Sensitivity Analysis and Application of Transducers. In: 5th International Summer School and Symposium on Medical Devices and Biosensors, Hong Kong, Peoples R China, June 01-03, pp. 85–88 (2008), ISBN: 978-1-4244-2252
6. Kasik, V., Adam, G.K., Garani, G., Smaras, N., Srovnal, V., Koziorek, J., Kotzian, J.: Design and development of embedded control system for a lime delivery machine. In: 10th WSEAS International Conference on Mathematical Methods and Computational Techniques in Electrical Engineering, Istanbul, Turkey, May 02-04, pp. 186–191 (2008), ISBN: 978-960-6766-60-2
7. Kasik, V.: FPGA based security system with remote control functions. In: Havlk, J., Uhl, J., Hork, Z. (eds.) 5th IFAC Workshop on Programmable Devices and Systems, Gliwice, Poland, November 22-23. IFAC Workshop Series, pp. 277–280 (2002), ISBN: 0-08-044081-9; Havlk, J., Uhl, J., Hork, Z.: Human Body Motions Classifications. In: IFMBE Proceedings EMBEC 2008 [CD-ROM]. Springer, Berlin (2008), ISBN 978-3-540-89207-6

8. Cerny, M., Martinak, L., Penhaker, M., et al.: Design and Implementation of Textile Sensors for Biotelemetry Applications. In: Conference Proceedings 14th Nordic-Baltic Conference an Biomedical Engineering and Medical Physics, Riga, Latvia, June 16-20, vol. 20, pp. 194–197 (2008), ISSN: 1680-0737, ISBN: 978-3-540-69366-6
9. Cerny, M., Penhaker, M.: Biotelemetry. In: Conference Proceedings 14th Nordic-Baltic Conference an Biomedical Engineering and Medical Physics, Riga, Latvia, June 16-20, vol. 20, pp. 405–408 (2008), ISSN: 1680-0737, ISBN: 978- 3-540-69366-6
10. Cerny, M., Penhaker, M.: The HomeCare and circadian rhythm. In: Conference Proceedings 5th International Conference on Information Technology and Applications in Biomedicine (ITAB) in conjunction with the 2nd International Symposium and Summer School on Biomedical and Health Engineering (IS3BHE), Shenzhen, May 30-31, vols. 1 and 2, pp. 110–113 (2008), ISBN: 978-1-4244-2254-8
11. Cerny, M.: Movement Monitoring in the HomeCare System. In: Dossel-Schleger (ed.) IFMBE Proceedings, vol. (25). Springer, Berlin (2009), ISBN 978-3-642-03897-6, ISSN 1680-0737

Author Index

Agapiou, George 302, 318, 543
Agha, Khaldoun Al 685
Aguado, Imanol 368
Agüero, Ramón 31, 43
Aguilar, Fernando López 356
Alam, Muhammad 380
Albillos, Santiago 31
Alonistioti, Nancy 112, 292, 318
Alonso, L. 604
Alonso-Zárate, J. 604
Antonopoulos, Angelos 346
Askoxylakis, Ioannis G. 216
Athanasopoulos, Nikos 543
Audsin, Dev Pramil 318
Avallone, Stefano 440

Bader, Faouzi 1, 11
Baldoni, Roberto 427
Bastos, Joaquim 57, 579
Batina, Lejla 254
Belesioti, Maria 302, 318
Bellec, Martial 464
Bendazzoli, Magda 68
Benikovsky, Jozef 699
Bkassiny, Mario 180
Bouchet, Olivier 484
Brida, Peter 699

Caban, Sebastian 388
Cabero, José María 673
Cabral, O. 57
Canada-Bago, J. 650
Carro-Calvo, L. 638
Castedo, Luis 388
Cendón, Bruno 31
Chaparro, Pedro 368
Chatzimisios, Periklis 88
Chelidonis, Konstantinos 318
Chochliouros, Ioannis P. 302, 318
Choque, Johnny 43
Choraś, Michał 451
Cidre, Gorka Rubio 356
Crespo, Pedro M. 618
Csertán, György 427

da Fonseca, Nelson L.S. 280
Dagiuklas, Tasos 555
Dainelli, Giulio 530
D'Alessandro, Salvatore 472
D'Amico, Antonio 506
D'Antonio, Salvatore 440
Del Ser, Javier 618, 626, 662
de Meulenaer, Giacomo 229
De Vogeleer, Karel 567
Diakonikolaou, George 302
Díaz, Francisco 22
Dimitriou, Nikos 530
Di Renzo, Marco 685
Doukoglou, Tilemachos 302, 318
Dounis, Lampros 555
Dreesen, Ralf 148
Duhamel, Pierre 685

Eickhoff, Ralf 136, 160
Ellinger, Frank 160
Elshaafi, Hisain 427
Erman, David 567

Fernández-Prieto, J.A. 650
Fernández, Yolanda 22
Ficco, Massimo 203
Fiedler, Markus 567
Fuentetaja, Rafael Gonzalez 464

Gadeo-Martos, M.A. 650
García-Naya, José A. 388
Garcia-Padrones, Laura 626, 662
Garrigas, Salva 368
Gazis, Evangelos 318
Georgas, Iraklis 543
Georgiadou, Evangelia 302
Germanus, Daniel 400
Gholam, Fouad 136, 171
Gil-Lopez, Sergio 626, 662
Gómez, David 31
Gönczy, László 427
Goni, Gilles 464
González, Ainara 368
Gonzalo, Álvaro 136
Görg, Carmelita 78

Gozálvez, Javier 368
Granelli, Fabrizio 68, 280
Grobe, Liane 484
Grygarek, Petr 769
Guglielmi, Michele 268
Gutierrez, I. 11

Hadzic, Senka 579
Henarejos, Pol 530
Hernaez, Mikel 618
Hernando, Gorka 673
Herrero, Jesús 31
Hołubowicz, Witold 451
Hutchison, David 415

Ikhlef, Ismahene 1
Iwaza, Lana 685

Janckulik, Dalibor 722
Javaudin, Jean-Philippe 464
Jayaweera, Sudharman K. 180
Jeckel, Sebastian 400
Jedidi, Azza 710
Jungeblut, Thorsten 148

Kartsakli, E. 604
Kastens, Uwe 148
Katsaros, Dimitrios 318
Katz, M. 604
Khelil, Abdelmajid 400
Kieffer, Michel 685
Kijonka, Jan 769
Kikiras, Panayotis 192
Kliazovich, Dzmitry 68, 280
Konecny, Jaromir 755
Könsgen, Andreas 78
Kotzian, Jiri 755, 769
Kousaridas, Apostolis 318
Kousaridas, Apostolos 292
Kozik, Rafał 451
Krejcar, Ondrej 722, 739, 755
Kuruc, Marian 755

Lafuente-Arroyo, S. 638
Lagunas, Eva 506
Landa, Itziar 662
Lee, Yong Ki 254
Li, Jianhui 484
Lindsay, Adam T. 415
Lippa, Tomas 755
Lodi, Giorgia 427
López, Fernando 368
López, José Manuel López 356
Low, Chor Ping 99
Lucas-Estañ, M^{a} Carmen 368

Machaj, Juraj 699
Madeira, Edmundo 280
Maldonado-Bascon, S. 638
Malheiros, Neumar 280
Maneros, Julen 368
Martini, Adamantini 192
May, John 216
Mehlführer, Christian 388
Miettinen, Antti P. 124
Mihailovic, Andrej 318
Minh, Hoa Le 484
Mizikakis, Christos 318
Mödeker, Jens 334
Modeker, Jens 318
Monserrat, Jose 368
Monteiro, V. 57
Moretti, Marco 530
Motalova, Leona 722
Mulcahy, Barry P. 427
Muñoz, Luis 43
Munro, Alistair 243

Nai, Igor 268
Nájar, Montse 506
Nazábal, Alfredo 171
Nguengang, Gerard 318
Nurminen, Jukka K. 124

O'Brien, Dominic 484
Ochoa, Idoia 618

Panaousis, Emmanouil A. 496
Paris, Javier Regidor 356
Pascual-Iserte, Antonio 518
Patouni, Eleni 112
Peña, Miguel Ángel 22
Penhaker, Marek 769
Perez-Garcia, Andres 268
Perez-Neira, Ana 530
Pérez, Susana 673
Pirmoradian, Mahdi 496
Politis, Christos 496
Politis, Ilias 555
Popescu, Adrian 567
Porrmann, Mario 148

Portilla-Figueras, A. 638
Portilla-Figueras, Jose A. 662
Prokop, Hynek 755

Rigas, Andreas 302, 318
Rodríguez, Arancha 31
Rodriguez, Jonathan 57, 380, 579
Romano, Luigi 203
Rückert, Ulrich 148
Rupp, Markus 388

Sacristán-Murga, Daniel 518
Said, Abdellatif 1
Sainz, Javier 31
Salcedo-Sanz, Sancho 638, 662
Santamaría, Ignacio 136, 171
Sanz, Aránzazu 31
Sfakianakis, Evangelos 302, 318
Sgora, Aggeliki 88
Siaterlis, Christos 268
Simpson, Steven 415
Singelée, Dave 254
Soltani, Faouzi 1
Spiliopoulou, Anastasia S. 302, 318
Stamoulis, George 192
Standaert, François-Xavier 229
Stankus, Martin 769
Suri, Neeraj 400

Taponecco, Lorenzo 506
Thies, Michael 148
Tonello, Andrea M. 472
Traganitis, Apostolos 216
Tralli, Velio 530
Tryfonas, Theo 216
Tsagaropoulos, Michail 555
Tsiakas, Panagiotis 543
Tykhomyrov, Vitaliy 590
Tyson, Gareth 415

Velasco, Juan R. 650
Velez, F. 57
Verbauwhede, Ingrid 254
Vergados, Dimitrios D. 88
Verikoukis, Christos 346, 604
Vía, Javier 136, 171
Voudouris, Konstantinos 543

Wagner, David 318, 334
Wang, Ting 99
Weis, Frédéric 710
Wolf, Mike 484
Wolf, Robert 160

Zaharis, Alexandros 192