Kostas Pentikousis
Oliver Blume
Ramón Agüero Calvo
Symeon Papavassiliou (Eds.)

32

Mobile Networks and Management

LNICST

First International Conference, MONAMI 2009
Athens, Greece, October 2009
Revised Selected Papers

Lecture Notes of the Institute
for Computer Sciences, Social-Informatics
and Telecommunications Engineering 32

Kostas Pentikousis
Oliver Blume
Ramón Agüero Calvo
Symeon Papavassiliou (Eds.)

Mobile Networks and Management

First International Conference, MONAMI 2009
Athens, Greece, October 13-14, 2009
Revised Selected Papers

Springer

Volume Editors

Kostas Pentikousis
VTT Technical Research Centre of Finland
Oulu, Finland
E-mail: Kostas.Pentikousis@vtt.fi

Oliver Blume
Alcatel-Lucent Deutschland AG
Bell Labs - Wireless Access
Stuttgart, Germany
E-mail: oliver.blume@alcatel-lucent.com

Ramón Agüero Calvo
Department of Communications Engineering
University of Cantabria
Santander, Spain
E-mail: ramon@tlmat.unican.es

Symeon Papavassiliou
School of Electrical and Computer Engineering
National Technical University of Athens
Zografou, Athens, Greece
E-mail: papavass@mail.ntua.gr

Library of Congress Control Number: 2009943843

CR Subject Classification (1998): C.2, C.2.3, H.5.4, K.4.4, K.6.5, G.4

ISSN 1867-8211
ISBN-10 3-642-11816-X Springer Berlin Heidelberg New York
ISBN-13 978-3-642-11816-6 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12842988 06/3180 5 4 3 2 1 0

Preface

The First International ICST Conference on Mobile Networks and Management (MONAMI) was held in Athens, Greece during October 13–14, 2009, hosted by the National Technical University of Athens. Through what we hope will be a long-lasting series of events, this new international conference aims at bringing together top researchers, academics, and practitioners specializing in the area of mobile network management. Multiaccess and resource management, mobility management, and network management have emerged as core topics in the design, deployment, and operation of current and future networks. Yet, they are treated as separate, isolated domains with very little interaction between the experts in these fields and lack cross-pollination. MONAMI 2009 offered the opportunity to leading researchers, industry professionals, and academics to meet and discuss the latest advances in these areas and present results related to technologies for true plug-and-play networking, efficient use of all infrastructure investments, and access competition.

MONAMI 2009 featured eight full papers and five short papers, which were selected after a thorough peer-review process based on their relevance to the scope of the conference and their technical merit. The overall acceptance rate was 50%. The contributing authors covered a range of topics in mobile networks and their management that are currently of high interest in the wireless research area. In particular, the revised papers included in this volume address handovers in multiaccess networks, along with the associated resource management issues; context and connection management for self-organizing networks; Future Internet architectures; and applications and algorithms. All papers were orally presented in a single-track format, which fostered active participation from all attendees.

The conference opened with a tutorial on "Mobility and Multiaccess in Emerging Internet Architectures" by Kostas Pentikousis. Antonio Puliafito opened the second day of the conference with a keynote speech on "Managing Heterogeneous Wireless Technologies: Objects Tracking and Services Development". Finally, the conference program included a panel session on "Energy Efficiency in Mobile Multiaccess Networks".

We acknowledge the vital role that the Technical Program Committee members and referees played during the review process. Their efforts ensured that all submitted papers received a proper evaluation. Finally, yet importantly, we thank Create-Net and the VTT Technical Research Centre of Finland for technically co-sponsoring the event.

November 2009 Kostas Pentikousis

Organization

Steering Committee Chair

Imrich Chlamtac	Create-Net, Italy

Steering Committee Co-chair

Kostas Pentikousis	VTT Technical Research Centre of Finland, Finland

General Chair

Kostas Pentikousis	VTT Technical Research Centre of Finland, Finland

Technical Program Committee Co-chairs

Oliver Blume	Alcatel-Lucent Bell Labs, Germany
Ramon Aguero	University of Cantabria, Spain
Symeon Papavasileiou	National Technical University of Athens, Greece

Web Chair

Jarno Pinola	VTT Technical Research Centre of Finland, Finland

Publicity Chair

Periklis Chatzimisios	TEI of Thessaloniki, Greece

Technical Program Committee

Ramon Aguero	University of Cantabria, Spain
Rui Aguiar	University of Aveiro, Portugal
Toufik Ahmed	University Bordeaux 1, France
Nadeem Akhtar	Centre of Excellence in Wireless Technology (CEWiT), India
Hussein Badr	Stony Brook University, USA
Oliver Blume	Alcatel-Lucent Bell Labs, Germany
Roksana Boreli	NICTA, Australia
Jochen Eisl	Nokia Siemens Networks, Germany
Raffaele Giaffreda	CREATE-NET, Italy
Jussi Kangasharju	University of Helsinki, Finland
Theo G. Kanter	Mid-Sweden University, Sweden

Timotheos Kastrinogiannis	National Technical University of Athens, Greece
Zhaojun Li	Fujitsu Labs, UK
Emmanuel Lochin	ISAE - LAAS-CNRS, France
Symeon Papavasileiou	National Technical University of Athens, Greece
Kostas Pentikousis	VTT Technical Research Centre of Finland, Finland
Henrik Petander	NICTA, Australia
Miguel Ponce de Leon	Waterford Institute of Technology, Ireland
Anand R. Prasad	NEC Corporation, Japan
Susana Sargento	University of Aveiro, Portugal
Haitao Tang	Nokia Siemens Networks, Finland

Table of Contents

Session 1: Handovers in Multiaccess Networks

Session 2: Context and Connection Management

Session 3: Future Internet

Session 4: Wireless Networking

Session 5: Algorithms and Applications

Session1:
Handovers in Multiaccess Networks

Handovers for Ubiquitous and Optimal Broadband Connectivity among Cooperative Networking Environments

Lambros Sarakis and George Kormentzas

National Centre for Scientific Research "Demokritos", Terma Patriarchou Grigoriou, Aghia Paraskevi 15310, Greece
{sarakis,gkorm}@iit.demokritos.gr

Abstract. The handover function is a key enabler for seamless mobility and service continuity among a variety of mobile/wireless access technologies supporting IP connectivity. The paper focuses on the key research challenges regarding inter-system handover operations among various radio cooperative networking environments (3G, WLAN, WiMAX and DVB) that are going to formulate future/near future business cases for both broadcasters and telecom operators in the context of a Fixed-Mobile Convergence (FMC) communications environment. In this context, relevant efforts from the IETF, IEEE 802.21, IEEE 1900.4, 3GPP and DVB are reviewed and incorporation of the IEEE 802.21 functionality inside the mobility management protocol stack is discussed.

Keywords: Heterogeneous Wireless Networks, Seamless Mobility, Media Independent Handovers.

1 Introduction

For several years, service providers, telecommunication equipment manufacturers and other vendors have faced the great challenge of networks and services convergence. Beyond the core fixed infrastructure, which has already largely migrated towards IP, the explosion of broadband and, simultaneously, the launch of 3G mobile networks have accelerated the synergy between heterogeneous networks, leading to an all-IP network. As a result, the challenge of delivering services like voice, data, content, video communications and video broadcasting can be realized in a ubiquitous manner.

The 3GPP and 3GPP2 have specified the IP Multimedia Subsystem (IMS) that aims to provide a workable and coherent solution for both fixed and wireless networks for delivering new generation converged services. This opportunity, stimulated also by the ETSI TISPAN [1], is rising fast and is largely contributing to the wide, although recent, recognition of IMS as the future direction of Fixed-Mobile Convergence (FMC). The FMC is a new dimension for the communications industry and presupposes the existence of multimode mobile terminals that are able to operate in virtually any mobile or wireless broadcasting communication network, such as 3G or DVB, and jump seamlessly to any WLAN or WMAN technology, including WiFi or WiMAX. Mobile terminals have to be capable of accessing different multimedia

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 3–13, 2010.

applications and advanced services while roaming across domains covered by different access technologies.

In the above context, the communications research and development community is investigating new ways to facilitate interworking among the various Radio Access Technologies (RATs) on providing seamless mobility and service continuity among them. A key enabling function for seamless mobility and service continuity among a variety of mobile/wireless access technologies supporting IP connectivity is the handover, in any IMS, pre-IMS, or combined network. In such environments, a strong constraint is the ability of multimode terminals to take full advantage of all added functionalities in the most profound way.

With respect to this, key challenges include the investigation, design, implementation and testing of inter-system handover operations among various radio cooperative networking environments (e.g., 3G, WLAN, WiMAX and DVB) that are going to formulate future/near future business cases for both broadcasters and telecom operators in the context of an FMC communications environment. As far as the optimization of the vertical handover operation is concerned, major contribution has been provided by the IEEE 802.21 working group, which has specified standardized mechanisms for closer-to-seamless handovers among 3GPP, 3GPP2 and several IEEE 802-based networks.

In this paper, which extends the work presented in [2], we discuss the challenges associated with the handover operation and review existing and emerging protocols and architectures that aim to support handovers between heterogeneous next-generation wireless systems. The relevant efforts of the IETF, IEEE, 3GPP and DVB are presented and the potential of IEEE 802.21 to deliver a framework for optimized handover operations is discussed.

The rest of the paper is organized as follows. Section 2 formulates the handover problem, while Section 3 gives a brief overview of current standardization efforts concerning inter-system handovers. Section 4 discusses open research and development issues related to inter-system handover. The components of a framework that aims to provide optimized handover operations are presented in Section 5, while conclusions are given in Section 6.

2 The Handover Problem Formulation

Mobility management is comprised of two components: location management and handover management. The former is needed to track the location of the terminal and, thus, enable packet reception. Handover management, on the other hand, is needed to keep the connections active while the mobile node moves from one location to another.

In general, handovers occur when a mobile node changes its Layer-2 network Point of Attachment (PoA), i.e., the end-point of a Layer-2 link between the mobile node and the network. Proper handover management must ensure that there is no noticeable interruption to running applications. This ultimate goal can be achieved if a number of sub-requirements are satisfied:

- Successful connection to target PoA: The mobile node must be able to connect to the target PoA. This presupposes that the mobile node is eligible for connection and that resources are available.

- Service continuity: After handover, the applications should be able to continue their operations without need for session reestablishment. For applications running on top of existing transport protocols like TCP and UDP this means that the applications must continue using the same logical connection; that is, the endpoint IP addresses must remain intact.
- Minimum handover delay and data loss: The time period during which the mobile cannot send or receive packets due to interface change must be kept to a minimum and actions must be taken to avoid or limit packet loss.

Handovers between links of the same technology are called intra-technology or horizontal handovers, while those occurring between different access technologies are called inter-technology or vertical handovers. The change of Layer-2 PoA (Layer-2 handover) may subsequently trigger reconfiguration of the IP address (Layer-3 handover) used by the mobile node as location identifier. This is the case when the current and the target PoAs are served by different Access Routers (ARs). Layer-3 handovers (whether horizontal or vertical) that occur between PoAs served by different ARs are called intra-system handovers when these ARs belong to the same access system, and inter-system handovers when the ARs belong to different access systems (usually distinct administrative domains).

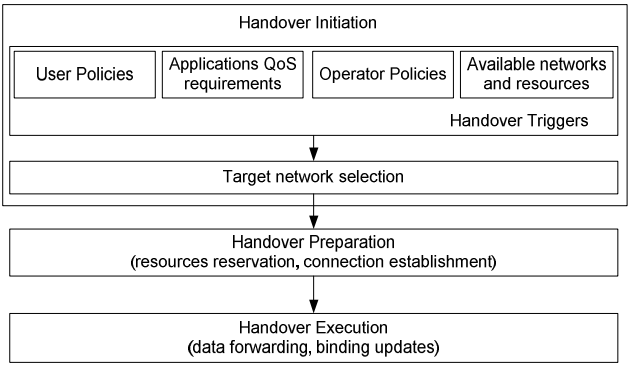


Fig. 1. Phases of the handover operation

Handovers take place during a session (i.e., when the terminal is in active mode; in idle mode, the switch of networks is usually called re-selection). The reasons triggering the handover as well as any pre-handover preparative actions should be clearly distinguished from the handover execution itself. In general, the handover operation can be separated in three phases (Fig. 1):

- Handover initiation: This refers to the decision mentioning the necessity for a terminal to change network. A reason could be either because the current network can no longer fulfill the end-user requirements or because it has been observed that another network could fulfill them in a better way. The outcome of this phase is the selection of the target network.
- Handover preparation: This phase involves preparations for the establishment of Layer-2 and Layer-3 connections to the target network, reservation of resources

and, if applicable, transfer of context (i.e., information regarding access control, QoS profile and header compression).

- Handover execution: This includes the events concerning the disconnection from the previous network and the connection to the target one. Furthermore, this stage addresses data forwarding from the previous network (if such a feature is supported by the mobility management protocol) and IP address binding update.

The role of handover initiation is to compile information about applications QoS requirements, user preferences, operator policies (reflecting also regulatory constraints) as well as available networks and take firm decisions on the need of the handover and the target network. The network selection is often treated as an optimization problem, the complexity of which increases with the number of the handover decision criteria and constraints and the number of available networks. Since handovers are costly (in terms of network signaling and processing power) and in many cases not seamless, decisions to switch networks must be made when it is deemed necessary.

However, in a rapidly changing and highly unpredictable mobile communication environment securing the handover decision and determining the right time to start handover preparation is not an easy task. Early handover decisions are usually due to incorrect predictions and lack of stable information (e.g., about signal strength deterioration or availability of other networks) and, thus, may not be optimal. Even worse, they may need to be cancelled before completion of the handover operation or shortly after (leading, for example, to the undesirable ping-pong effect). Mature handover decisions, on the other hand, may come too late to allow for efficient handover preparation; this can cause increased handover delay and packet loss. Clearly a trade-off between the two approaches is needed.

The next phase in handover operation, namely the handover preparation, deals with the actions that can be taken in advance to mitigate the impact of handover execution on applications' performance. Compared to handover initiation, this step depends more heavily on the mobility management protocol involved in handover (which, in turn, may depend on the type of the handover and the involved RATs). For Layer-2 handovers this phase addresses resource allocation to the target network and Layer-2 authentication and association. For Layer-3 handovers, it may further facilitate movement detection and expedite the configuration of the IP address used in the target network. Additional actions include preparations for data forwarding from network nodes of the previous network to the AR of the target network.

The last step in handover operation is handover execution, during which the mobile node connects to the target network. The network entities in previous and target networks may, furthermore, cooperate to forward data to the mobile node until location update is completed. As soon as this happens, resources are released in previous network and normal data forwarding to the mobile terminal is resumed.

Handover mechanisms that are able to provide seamless mobility are quite complicated and depend on functionality that spans across several layers in the networking protocol stack (from physical to network and application). Thus, smooth cooperation of these functions is essential for efficient realizations targeting complete system solutions.

3 Brief Overview of Recent Standardization Efforts Concerning Inter-system Handovers

3.1 IETF Efforts

The basis for terminal mobility management in IETF is provided by Mobile IPv4 (MIPv4) [3]. MIPv4 works by allocating two addresses to a Mobile Terminal (MT): a permanent global address (home address) belonging to the address space of the home network, and a temporary local address (care-of-address) allocated to the MT at the visiting network (usually this address is provided by a router called foreign agent). Traffic destined to the MT is always routed to the home domain and is collected by a router called home agent. This router, subsequently, tunnels the packets to the foreign agent based on the mapping between MT home and care-of-address is has previously created. After appropriate processing of the packets (tunnel decapsulation), the foreign agent forwards them to the MT.

Mobile IPv6 (MIPv6) [4] introduces several advantages over MIPv4 that aim to optimize the communication between correspondent nodes and MTs. In MIPv6, foreign agents are not needed, route optimization is supported as part of the basic functionality, and there is inherent support for coexistence of route optimization and routers performing "ingress filtering". However, direct communication between correspondent nodes and MT presupposes that the former are able to support mobility-aware operations.

The Mobile IP schemes just presented introduce significant handover latency due to procedures like movement detection, new care-of-address configuration and location update. This latency is often unacceptable for real-time applications. Two protocols have been proposed to reduce the handover latency of MIPv6: Fast MIPv6 [5] and Hierarchical MIPv6 [6]. The former is an enhancement to the MIPv6 protocol that mitigates handover delay by involving communication between the previous and the next access routers in the foreign network, while the latter adds extensions to MIPv6 that support localized mobility management (i.e. management of topologically small movements within an access network). Hierarchical MIPv6 and Fast MIPv6 have complementary capabilities and functions, and, thus, can be used in parallel to further improve the handover experience. Combination of these schemes is known as Fast Hierarchical MIPv6 [7].

The protocols described thus far are terminal-based in the sense that the MT needs to be provisioned with functionality to perform handover and location management signaling when it moves between access network subnets. Recently, there was an interest from IETF to define a network-based localized mobility protocol (NETLMM[8,9]) that would allow MTs to move between subnets within the same access network (operational domain) without requiring changes in the IPv6 protocol stack.

The protocol that was specified within the NETLMM Working Group, called Proxy MIPv6 [10], introduces functionality for first-hop routers and special nodes in the access network called Local Mobility Anchor Points (LMAPs), which act as localized home agents. The first-hop router performs mobility management on behalf of the mobile by providing, in cooperation with the LMAP, router advertisements that make the MT believe it is still connected to the home network (and thus it can keep the same address). After detecting the movement of the MT, the first-hop router initiates signaling with the LMAP to update the route to/from the MT's home address.

Another approach to handle mobility in IP-based networks is the Session Initiation Protocol (SIP) [11]. SIP is an application-layer control (signaling) protocol for the creation, modification and termination of sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP addresses mobility at the application layer, and while it is capable of performing location management (through appropriate binding of SIP addresses to current location, namely IP address) it requires session reestablishment every time the MT changes its network address.

3.2 IEEE Efforts

The intention of the IEEE 802.21 standard [12] is to provide generic link layer intelligence independent of the specifics of mobile nodes or radio networks. As such, the IEEE 802.21 is intended to provide a generic interface between the link layer users in the mobility-management protocol stack and existing media-specific link layers, such as those specified by 3GPP, 3GPP2 and the IEEE 802 family of standards.

The standard specifically describes a logical entity (called Media Independent Handover Function - MIHF) residing between the link and upper layers, which provides three services to Media Independent Handover (MIH) users [12]:

- The Media Independent Event service, which detects events and delivers triggers from both local as well as remote interfaces;
- The Media independent Command service, which provides a set of commands for the MIHF users to control handover relevant link states;
- The Media Independent Information service, which provides the information model for query and response, thus enabling more effective handover decisions across heterogeneous networks.

Incorporation of IEEE 802.21 services in terminal and network nodes has the potential of optimizing the initiation and preparation phases of the handover operation and, thus, providing enhanced service experience to mobile users.

Optimized radio resource usage in composite wireless radio environments cannot be achieved unless efficient handover decision making is supported by both the network and the terminals. Towards this direction, a Working Group inside the IEEE (IEEE 1900.4 [13]) took action to address the broader problem of dynamic network re-configurability, one key enabler of which can be the handover operation (the standard further addresses two other key enablers: dynamic spectrum assignment and dynamic spectrum access). The standard specifies the building blocks that are necessary, both at the network and the terminal's side, to support distributed reconfiguration decision making. The addressed system architecture is comprised of three building blocks [14]:

- Network Reconfiguration Manager (NRM) entity that facilitates the derivation of network policies, which constrain the resource selection strategies of user terminals;
- Terminal Reconfiguration Manager (TRM) entity with facilities for enabling user devices to perform a (distributed) self-management-based optimization of their respective resource usage strategies subject to policies imposed by the NRM;

- Radio Enabler (RE) entity, which addresses the transfer of information between the network and the terminal reconfiguration management entities.

The TRM and NRM exchange context information (e.g., terminal and network capabilities and measurements, terminal location, user preferences and application QoS requirements), the collection of which is supported by appropriate measurement collectors at both the terminal and network sides. The NRM formulates reconfiguration (e.g., handover) policies and constraints, and forward them to the TRM via the RE. This is the first level of decision making; the second level of this network/terminal distributed process involves decisions taken by the TRM based on the policies and constraints received by the NRM.

3.3 3GPP Efforts

Future wireless networks will work on a cooperative manner and support mobility of terminals among heterogeneous systems/technologies. With respect to this challenge, the 3GPP is addressing the evolution of its system architecture (System Architecture Evolution – SAE), in conjunction with the evolution of the access system (Long Term Evolution – LTE), in order to deliver an evolved network able to support a variety of different access systems and access selection based on combinations of operator policies, user preferences and access network conditions. In this context, mobility-related requirements of the new architecture include the following [15]:

- Mobility management functionality shall be responsible for mobility within the evolved 3GPP system, as well as between that and different types of access systems including for example WiMAX and WiFi;
- The evolved 3GPP mobility management shall allow the network operator to control the type of access system being used by a subscriber;
- Mobility procedures within 3GPP access systems and between 3GPP and non-3GPP access systems shall provide seamless operations of both real-time (e.g. VoIP) and non real-time applications and services by, for example, minimizing the packet loss and interruption time.

3GPP leverages on network-layer mobility management protocols from IETF for its evolved network architecture. The 3GPP SAE paradigm shows that mobility management protocols, like MIPv4, MIPv6 and its extensions (e.g. Hierarchical MIPv6 and Proxy MIPv6), have been considered as candidate components for mobility between existing and emerging heterogeneous networks.

3.4 DVB Efforts

Taking into consideration the support for mobile Digital TV, ETSI introduced the DVB-H specification, which substantially comprises of a set of extensions to DVB-T which are oriented to handheld use. DVB-H inherits all the benefits of its predecessor and adds new, mobile-oriented features, focusing on IP datacasting and including better mobility and handover support, adaptive per-service error protection and power saving capabilities.

IP Datacast (IPDC) over DVB [16,17] is an end-to-end broadcast system for delivery of any type of digital content and services using IP-based mechanisms optimized

for devices with limitations on computational resources and battery. An inherent part of the IPDC system is that it comprises of a unidirectional DVB broadcast path that may be combined with a bi-directional mobile/cellular interactivity path. IPDC is thus a platform that can be used for enabling the convergence of services from broadcast/media and telecommunications domains (e.g., mobile/cellular).

In order that all developed services can be deployed in a uniform basis a lot of standardization effort is devoted regarding architecture and software issues. Towards this direction, the DVB CBMS (Convergence of Broadcasting and Mobile Services) Working Group has set an initial framework for use cases and services of DVB-H [16] and illustrated the way the components in IP Datacast over DVB-H work together [17].

Convergence of Internet and Broadcasting Systems [18] is at the moment at its infancy with many efforts resulting out of European driven initiatives. In most cases, vertical handover decisions are driven by overlooking gateway and/or management entities that 'decide' on the access network the user should be attached.

4 Open Research and Development Issues Related to Inter-system Handover

Legacy systems were designed and optimized without interoperability in mind, thus resulting in isolated communication networks with very tight bounds in geographical and service mobility. However, the advents of Beyond 3G have fuelled collaborative activities within the IEEE, IETF and 3GPP to construct a logical bridge between legacy systems to promote global roaming. Likewise, there has been recent interest from the broadcasting world to additionally integrate broadcasting services on a common service platform to address future market scenarios, thus raising significant future design challenges which include:

- New compatibility requirements to the IEEE 802.21 MIH architecture to provide cooperative dialogue with the DVB networking world;
- The seamless challenge (vertical handover involving DVB is a technical challenge) since the networks may not be synchronized, and even the content stream may not be identical (i.e., for the broadcasting case, the compression rates may not be the same).

The optimized operation of all phases of a handover procedure taking also into account downlink-only technologies like DVB that create new business cases, constitutes an open R&D issue that could also affect the evolution and well establishment of Next Generation Networks (NGNs) that are going to stimulate FMC vision. Obviously, this operational optimization is tightly related to the dynamics of all handover phases (initiation, preparation, execution), as well as the interfacing of handover operation to upper service layers that assist seamless mobility and service continuity through MIP and SIP.

A great research challenge that builds on top of recent research advances on both the handover procedure phases and upper service layers, is related with the investigation, design, implementation, testing and standardization of enabling technologies for optimized inter-system handovers operations among various radio cooperative networking environments (like 3G, WLAN, WiMAX and DVB) that are going to

formulate future/near future business cases for both broadcasters and telecom operators in the context of a FMC communications environment.

Alongside with this research challenge, 3GPP, IEEE 802.21, IEEE 1900.4 and IETF provide new functional blocks that aim to facilitate further inter-system handover procedures. However, from a systems perspective view, the ability of these functions to cooperate in a harmonized fashion still has to be evaluated. Equally important is to investigate the interactions among these functions and the functions of upper layers (MIP/SIP) in any IMS, pre-IMS, or combined network.

Furthermore, the functional requirements for integrating other emerging technologies like DVB-T/H have to be identified and evaluated in an explicit manner. Towards this direction, a Task Group inside IEEE 802.21 has been recently formed to start the IEEE P802.21b project, which aims to investigate required extensions to the IEEE 802.21 standard to support handovers between 3GPP or IEEE 802, and DVB downlink-only technologies. DVB and other down-link only technologies pose extra challenges since a bi-directional physical link is not always available and services are primarily broadcasting-oriented [19].

5 Components of a Framework for Optimized Handover Operations

As already mentioned in subsection 3.2, IEEE 802.21 provides generic link layer intelligence, which is independent of the specifics of mobile nodes or radio access networks. This is done by the introduction of the MIHF logical entity residing between the link (Layer-2, L2) and upper layers (Layer-3, L3, and above) of the mobility management protocol stack. MIHF exploits triggers from the link layer to facilitate handover initiation (network discovery, network selection, handover negotiation) and handover preparation (L2 and IP connectivity). Issues like handover control, handover policies, algorithms involved in handover decision making and handover execution are not covered by the standard [12].

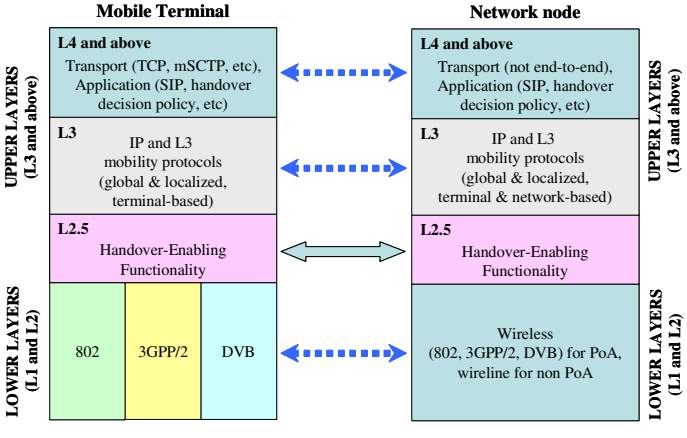


Fig. 2. IEEE 802.21-based mobility management protocol stack

The logical placement of the MIHF (identified as handover-enabling functionality residing at Layer-2.5, L2.5) within a mobility management protocol stack that is intended to deliver optimized handover operations (i.e., handover operations that rely on link-layer intelligence and global network information to realize closer-to-seamless experience) is illustrated in Fig. 2. The mobility management protocol stack presented in this figure is compatible with the hierarchical mobility management foreseen for next-generation networks (addressing mobility at both local and global levels) and the need to incorporate network-based mobility solutions. It is also compatible with the necessity to incorporate functions at Layer-2.5 for handover initiation and preparation, and functions at higher layers for handover decision policies (i.e., access selection), which can be provided, for example, by IEEE 1900.4. Mobility management in the network layer and above is addressed by IETF protocols (e.g., MIP, Proxy MIP, mSCTP [20] and SIP).

According to IEEE 802.21, a mobile terminal featuring MIH functionality may communicate with peers in the network. When the peer resides inside the same network entity as the mobile terminal's point of attachment, the communication between the two peers can be done through L2 message exchange (L2 transport has been specified for several IEEE 802 based technologies). However, if the peer is located deeper in the network, the communication takes place over Layer-3. When the mobile node is connected to a 3GPP network the communication with the peer is done only over Layer-3.

The mobility management protocol stack depicted in Fig.2 can be used as a basis for a framework targeting handover operations that are able to provide end-users with closer-to-seamless handover experience. This framework will rely on a) appropriate entities at the network side hosting functionality for mobility management (different entities may be responsible for different parts of the functionality presented in Fig. 2) and b) on efficient communication between the network entities themselves as well as between these and the MT.

6 Conclusions

A key Fixed-Mobile Convergence driver is to provide ubiquitous high-speed wireless connectivity to mobile multimode terminals using cost-effective techniques. In such an environment, it will be necessary to support seamless handover without causing disruption to ongoing sessions. The achievement of this vision requires cooperative radio networks that share system information and assist in handover events resulting in a seamless end-user experience irrespectively of the application at hand.

This paper elaborated on the functionality that is needed for the initiation, preparation and execution phases of the handover operation, reviewed current standardization efforts regarding support for vertical handovers and presented the components of an optimized handover framework that is based on emerging technologies proposed by the IEEE and the IETF. This framework, which is built around the concept of IEEE 802.21, combines the strengths of protocols residing at different layers of the mobility management protocol stack and targeting different phases of the handover operation. Application of such a framework is promising to deliver optimized handover operations that constitute potential business cases for both Telecom Operators and Broadcasters in the context of the emerging Fixed-Mobile Convergence communications environment.

Acknowledgments. The work presented in this paper has been undertaken in the context of the project INFSO-ICT-216006 HURRICANE (Handovers for Ubiquitous and optimal bRoadband connectIvity among CooperAtive Networking Environments). The project has received research funding from the European seventh Framework Programme. The authors would like to acknowledge the contributions of their colleagues from the HURRICANE consortium.

References

[1] ETSI TISPAN, http://www.etsi.org/tispan/
[2] Sarakis, L., Kormentzas, G.: Handovers for Ubiquitous Connectivity in Next Generation Wireless Systems. In: Proc. ICT-MobileSummit 2008, Stockholm, June 2008, pp. 1/8–8/8 (2008)
[3] Perkins, C. (ed.): IP Mobility Support for IPv4, RFC 3344, IETF (August 2002)
[4] Johnson, D., Perkins, C., Arkko, J.: Mobility support in IPv6, IETF, RFC 3775 (June 2004)
[5] Koodli, R. (ed.): Fast handovers for mobile IPv6, RFC 4068, IETF (July 2005)
[6] Soliman, H., et al.: Hierarchical mobile IPv6 mobility management (HMIPv6), RFC 4140, IETF (August 2005)
[7] Jung, H., et al.: Fast Handover for Hierarchical MIPv6 (F-HMIPv6), Internet Draft draft-jung-mobopts-fhmipv6-00.txt, IETF (October 2005)
[8] Kempf, J. (ed.): Goals for Network-Based Localized Mobility Management (NETLMM), RFC 4831, IETF (April 2007)
[9] Kempf, J. (ed.): Problem Statement for Network-Based Localized Mobility Management (NETLMM), RFC 4830, IETF (April 2007)
[10] Gundavelli, S. (ed.): Proxy Mobile IPv6, RFC 5213, IETF (August 2008)
[11] Rosenberg, J., et al.: Session Initiation Protocol, IETF, RFC 3261 (June 2002)
[12] IEEE Std 802.21-2008, IEEE Standard for Local and Metropolitan Area Networks—Media Independent Handover Services (January 2009)
[13] IEEE P1900.4 Working Group on Architectural Building Blocks Enabling Network-Device Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks, http://grouper.ieee.org/groups/scc41/4/index.htm
[14] IEEE Std 1900.4-2009, IEEE Standard for Architectural Building Blocks Enabling Network-Device Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks (February 2009)
[15] 3GPP TR 23.882, 3GPP System Architecture Evolution: Report on Technical Options and Conclusions (Release 8), v8.0.0, 3GPP (September 2008)
[16] ETSI TR 102 473, Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Use Cases and Services, v1.1.1, ETSI (April 2006)
[17] ETSI TR 102 469, Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Architecture, v1.1.1, ETSI (May 2006)
[18] Convergence of Internet and Broadcasting Systems, Special Issue. IEEE Network Magazine 21(2) (March/April 2007)
[19] Miloucheva, I., et al.: Seamless Handover For Unidirectional Broadcast Access Networks In Mobile IPv6. Journal of Communications 2(6) (November 2007)
[20] Stewart, R., et al.: Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration, RFC 5061, IETF (September 2007)

OpenMIH, an Open-Source Media-Independent Handover Implementation and Its Application to Proactive pre-Authentication

Yoann Lopez and Eric Robert

THALES Communications
Advanced Information Technologies Department
160 boulevard de Valmy - BP 82 - 92704 COLOMBES Cedex – France
{yoann.lopez,eric.robert}@fr.thalesgroup.com

Abstract. Enabling a seamless experience for mobile users while dealing with multi-access networks is a great challenge for wireless access providers. Towards this goal, the IEEE 802.21 Working Group is elaborating the needed mechanisms and the standardization effort has led to a Media Independent Handover Services (MIHS) framework that is now ready for deployment. However, no public implementation of those mechanisms is available yet. This paper presents OpenMIH, an implementation of MIHS and an illustrative scenario for proactive pre-authentication using off-the-shelf components for authentication. In particular, it demonstrates how network selection and handover preparation can be leveraged by such an implementation.

1 Introduction

Since the early 80s, IP networking deployment has driven the growth and the transformation of the global Internet. These last couple of years, we have been witnessing an unprecedented evolution that brings to market a wide spread of powerful and affordable mobile devices. In addition to their large set of isolated functional features, these devices embed an increasingly rich set of networking interfaces for wireless communications such as Wi-Fi, UMTS/GSM, DVB or WiMaX. This proliferation of personal and portable devices has drastically changed the usage model for the Internet. Needs for mobile IP networking solutions able to achieve seamless mobility across heterogeneous access networks are more than ever a reality.

Radio resource management mechanisms together with mobility protocols [1][2][3] provide session continuity when moving across different IP networks, possibly using multiple simultaneous radio interfaces. This class of solutions provides ways to manage handovers and, associated with make-before-break mechanisms, may help reducing the handover delay and the impact on applications. Nevertheless, they are not sufficient for achieving the ABC paradigm [4] that states that a mobile user may access the Internet from anywhere, at anytime and at the lowest possible cost, may it be in terms of access price or in terms of energy consumption. To do so, they must be coupled with correct network discovery and selection which permit to timely

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 14–25, 2010.

trigger a handover from one network to another when the mobile environment changes.

Facing the problem of correct and timely-significant network selection, the IEEE 802.21 Working Group (WG) [5] was created in order to propose common services for handover management. A handover, may it be horizontal (between homogeneous radio technologies) or vertical (between heterogeneous technologies), requires the following successive steps: handover initiation, preparation, and execution. The outcome of the IEEE 802.21 WG is the Media Independent Handover Services standard (MIHS) [6] which describes an architecture to lever handover initiation and preparation, while exhibiting an abstract interface for controlling an arbitrary number of heterogeneous radio interfaces. This interface, offered to mobility mechanisms, makes it possible to perform handover execution in a media-independent manner.

For achieving ABC and seamless mobility, the three handover steps must carefully been addressed. Though, in our work, we specifically focus on the purpose of MIHS - namely the handover initiation and preparation - whilst handover execution is not particularly addressed. In this context, the outcome of our work is twofold. First, we believe that experimental evaluation of MIHS is crucial for the networking community and we accordingly propose OpenMIH, a publicly-available open-source implementation of MIHS. Second, we demonstrate the benefits of this implementation for handover preparation in a secure handover experimental setup.

Deployment of MIHS is expected 2009-2010 but, to the best of authors' knowledge, there is not yet any publicly available implementation. There seems to be a need for such an implementation and related work has already been reported.

The remainder of this paper is structured as follows: first, we introduce the IEEE Media Independent Handover Services standard, its architecture and main components. Then, we introduce OpenMIH, an open-source implementation of MIHS. Designed with extensibility in mind, its purpose is to be a support for experimentation of mobility mechanisms in heterogeneous environments. Finally, we illustrate the functionalities of this implementation by proposing a specific scenario that demonstrates how to improve handover decision in a secure mono-technology Wi-Fi-based environment using proactive pre-authentication.

2 Related Work

In [7], a partial implementation of MIHS is presented for SIP-based VoIP handoff optimization. The reported features include network discovery, network selection, preconfiguration, pre-authentication, and proactive handover using MIH services. Yet, this implementation does not aim at being publicly disclosed and no information on its internal structuring, beyond the general MIH structure, is available. Unified Link Layer API (ULLA) [8] solution aims at facilitating the implementation of network-aware applications by offering a SQL-like request service to obtain information on current link conditions. As such, ULLA can be considered as a very early MIH Information service (e.g., it only considers presently attached RATS and do not take into account surrounding connections opportunities). Yet, it is not based on any standard since it was released in 2006 when IEEE 802.21 was not published. Finally, a GNU/Linux 802.21 implementation has been reported in [9]. This implementation

focuses on the support of several access technologies including IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMax) or IEEE 802.3 (Ethernet), using off-the-shelf Linux capabilities. It has been demonstrated for adaptive services such as VoIP. Our approach is complementary and aims at providing a generic MIHS framework encompassing the standard's communication model, transport and state machines.

Besides these implementation activities, it is worth mentioning the initiative for integrating a MIH model to the ns-3 network simulator [10]. In this model, the implemented services and interfaces are quite close to the standard but still, its primary use is for simulation purpose and it cannot be used to evaluate real applications.

3 Media-Independent Handover Services

The Media-Independent Handover Services (MIHS) standard proposed by the IEEE 802.21 WG aims at enabling seamless handover when moving across heterogeneous networks, including IEEE 802 and cellular networks. Horizontal handovers mechanisms are already defined for individual radio technology (e.g. IEEE 802.11r [11] for Wi-Fi, IEEE 802.16e [12] for WiMaX) but when it comes to vertical handovers, MIHS brings the necessary interoperability for seamless handover operations. The outcome of the IEEE 802.21 WG is therefore a generic architecture that provides common services for heterogeneous link management and that harmonizes the work performed by the different IEEE 802 WGs on handover optimizations. Expectations of the standard include optimum network selection, mobile-initiated and network-initiated handovers as well as low-power operations for multi-radio devices.

MIHS is an architectural framework for handover management that takes advantage of a set of MIH Functions (MIHF) available at different network locations. Actually, the MIHS standard states that any equipment in the network may provide handover-enabling capabilities by the adjunction of a MIHF. Those so-called MIH network entities exchange information together, complying with the MIH communication model depicted in Figure 1. Interactions between MIH network entities may be categorized as follows:

- *Mobile to Network (M2N)*: these communications occur in case of a mobile-controlled handover. MIH exchanges are initiated by the mobile node's MIHF.
- *Network to Mobile (N2M)*: communications for network-controlled handover.
- *Network to Network (N2N)*: communications between network-side equipments. This is the case when check for resource availability is needed during a handover.

The focus of the MIHS standard is to specify the MIH communication model, to elaborate the MIHF architecture, its services and its Service Access Points (SAPs) and associated primitives. Depending on its role in the communication model, a MIH network entity may interact locally with a combination of several heterogeneous radio interfaces (link layers) and with a variety of MIH Users (MIHU). Link layers provide a common interface to the MIHF in order to determine their state and control them regardless of the underlying radio technology. MIHUs may be any application using the MIHF and typically are mobility management or resource management functions.

For example, a MIH mobile node may embed a set of heterogeneous radio interfaces similarly abstracted to a set of MIHUs, while a Point-of-Attachment (PoA) may only avail the control of its only interface. Similarly, a Point-of-Service (PoS) may not have any MIH-controllable link layer but may nonetheless exchange information with a mobile node during a handover.

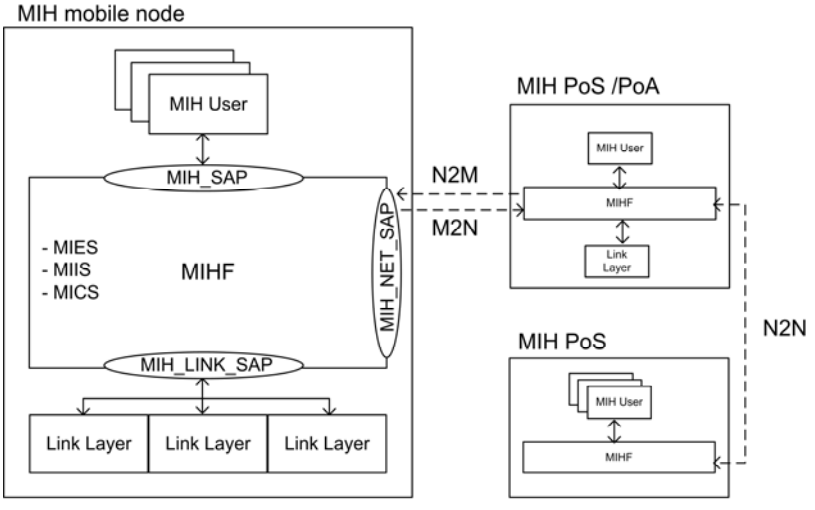


Fig. 1. Network entities in the MIH communication model. Plain arrows denote local interactions within MIH network entities while dashed arrows identify remote communications between MIH Functions.

Three services are of particular interest for enhancing handovers between heterogeneous access links.

- *Media Independent Event Service (MIES)* that provides event classification, event filtering and event reporting corresponding to dynamic changes in link characteristics, link status, and link quality.
- *Media Independent Command Service (MICS)* that enables MIH Users to manage and control link behavior relevant to handovers and mobility.
- *Media Independent Information Service (MIIS)* that provides details on the characteristics and services provided by the serving and neighboring networks. The information enables effective system access and effective handover decisions.

Taking a mobile-controlled handover as an example, the MIHUs (e.g. mobility manager) of a given MIH mobile node equipped with multiple network interfaces of arbitrary type, would be served by a combination of the abovementioned services provided by the local MIHF though the MIH_SAP interface. This interface enables the management and control of the state of underlying interfaces in a unified way through the MIH_LINK_SAP interface. Additionally, the MIH_NET_SAP interface permits the invocation of services provisioned by remote MIHFs. For the understanding of the overall architecture, it is worth mentioning that the scope of the MIHS standard does

not include the link layers; and that media-specific amendments are proposed by each respective standardization body for their management.

4 OpenMIH implementation

OpenMIH [13] is an implementation of the latest approved MIHS standard and partially implements a MIHF conformant with the standard. As it is an implementation of a MIHF and its associated MIH services, it is suited to be embedded in any MIH network entity described in the MIH communication model and may run on constrained devices (e.g. mobile handheld) as well as on high-end servers (e.g. operator's mobility server). The OpenMIH implementation packages a software architecture for the MIHF, the MIH Service Access Points (SAPs), data types, the MIH communication protocol and associated MIH messages defined in the standard.

OpenMIH is a configurable network daemon, developed in C language as a single process and has been tested on standard GNU/Linux operating systems on x86 architectures. The software architecture of an OpenMIH MIHF is depicted in Figure 2.

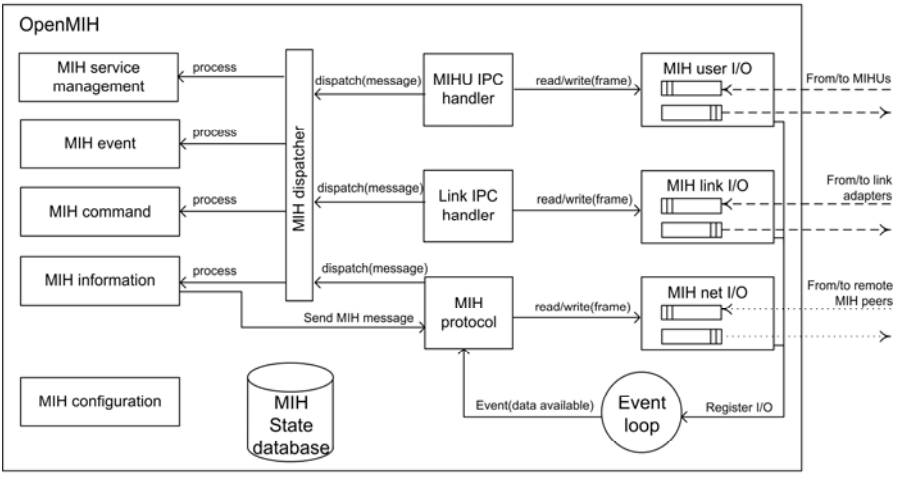


Fig. 2. OpenMIH detailed software architecture: dotted arrows denote MIH messages (encapsulated for transport), dashed arrow depict local IPC messages while solid arrows represent synchronous function calls.

As described in the standard, a MIHF may communicate with a large set of components, either locally (e.g. with MIHUs) or remotely (e.g. with remote MIHF peers) and may therefore involve a fair amount of network I/O (Input/Output) operations. Among different I/O strategies [14], asynchronous (or non-blocking) I/O has been selected because it is a technique specifically targeted at handling multiple concurrent I/O requests efficiently. As a consequence, the core of the architecture is an asynchronous event loop. Each I/O module corresponding to MIHF interfaces may create a socket (e.g. TCP, UDP or raw socket) and is able register a callback function that the

event loop may call when activity is reported on the corresponding socket file descriptor. Most modern operating systems provide this flexible way to handle concurrent I/O and, for our purpose, we selected the *libevent* library [15] that encompasses various scalable backend mechanisms to loop through socket file descriptors (e.g. `select`, `poll` and `epoll`).

The event loop monitors the activity of the I/O modules described below and notifies the respective handlers when data is available:

- *MIH user I/O* is designed to serve a set of MIHUs that may concurrently invoke different MIHF services, either locally or remotely. The multiplexing of incoming requests are offered by a TCP server and message passing is used as a convenient way for Inter-Process Communications (IPC) [16]. For differentiating the MIHUs invocations to local MIH services or to a remote MIHF peer, the *MIH IPC handler* is able retrieve MIH service ID (SID), action ID (AID), operation code (opcode) and the destination MIHF ID (see [6] for details on those data types) in the IPC frame. Then, dispatching to the relevant modules is straightforward.
- *MIH link I/O* provides handlers for the various link adapters that are designed as separate processus. In order to feature IPC, we use bi-directional message passing through TCP sockets. Link adapters implement the media-specific SAPs primitives required for the interoperability with the MIHS standard. The link adapters are similar to the Link Information Collector (LIC) introduced in [9]. Due to the unavailability of link drivers implementing media-specific SAPs and primitives [17][18], we use a simulated link adapter and *link IPC handler* provides the unambiguous mapping of those primitives with MIH_LINK_SAP primitives.
- *MIH net I/O* manages concurrent bi-directional transport and encapsulation of unitary MIH frames with remote MIHF peers. Transport of MIH messages may be accomplished in a media-dependent (OSI layer 2) or in a media-independent way (OSI layer 3 and upper). Depending on the radio capabilities, L2 transport may be performed over data plane or management plane. Similarly, transport over upper layers is proposed by the IETF MIPSHOP WG [19]. As appropriate transport depends on the type of message that needs transferring and as *MIH net I/O* is agnostic to the MIH message type, it provides an interface to set the necessary transport parameters. At the current state, the implementation offers transport at L3 over TCP and UDP.

For sake of clarity, all synchronous functions calls between the software modules have not been depicted in Figure 2. Nevertheless, we give indications of the interaction of each module with the others in the following descriptions:

- *MIH management* module allows runtime management of the MIHF modules. In particular, it includes MIH discovery, registration and event subscription.
- *MIH event* module handles the dispatching of local and remote link events to local MIHUs according to their event subscription.
- *MIH command* module handles MIH command requests from MIHUs or remote MIHF peers and maps them onto link commands thanks to the *link IPC handler*.
- *MIH information* module handles MIH information requests from MIHUs or remote MIHF peers. It maintains dynamic information about the network environment and provides an interface for information querying and filtering. The

MIHS standard indicates two ways of representing the information elements: Type-Length-Value (TLV) and Resource Description Framework (RDF) [20]. Associated identifiers allow the mapping of information elements between both representations. For the implementation, a RDF description has been selected for its extensibility features. Among the several engines for RDF parsing and information querying [21], we selected the *Redland* RDF libraries [22] that support RDF parsing as well as the SPARQL query language [23].

- *MIH protocol* module keeps track of the ongoing MIH exchanges with remote MIH peers by means of MIH transactions and MIH Finite State Machines (FSM). Upon the reception of a MIH frame from the *MIH net I/0,* it is deserialized into a MIH message structure. This data structure exhibits all the message's characteristics, namely the MIH fixed-length header, and a list of its associated variable-length TLVs. Based on this information, the MIH protocol is able to lookup an ongoing transaction, to drive its associated FSM and to trigger needed actions, (e.g. restart retransmission timer, send acknowledgement). Reversely, it proposes an internal interface to MIH services for sending MIH message to remote MIHF peers. In this case, the *MIH protocol* takes care of initiating a new transaction with a remote MIHF peer and provides a hook for asynchronous notification of the transaction's completion. As hinted in the description of the *MIH net I/O* module, MIH frames may be transmitted by means of different mechanisms depending on their required reliability. An overview of transmission strategies using UDP, TCP and GIST signaling protocol with various settings for retransmission and acknowledgements can be found in [24] and is insightful for configuring the transport parameters. For our purpose, the implementation uses unreliable UDP transport for MIH event service messages and reliable TCP transport for other services.
- *MIH configuration* module is used for selecting MIH services and configuring their attributes at startup. It is described in a straightforward YAML file that is parsed using *libyaml* libraries [25].
- *MIH states* database is a global structure that is shared within the MIHF and that maintains states between the calls of the various components. In particular, it maintains the capabilities of the MIHF, the available events, the MIHUs list, handlers to the link adapters, the MIHF peer table and their individual characteristics.

5 Proactive Pre-authentication Using OpenMIH

In order to illustrate the capabilities of OpenMIH in an integrated architecture, we propose to tackle the challenge of handover preparation when moving across a homogeneous Wi-Fi network requiring strong mutual authentication. Towards this objective, pre-authentication aims at reducing handover delay and resulting packet loss by initiating authentication procedures with possible candidate PoAs while still remaining attached to the serving one. This way, the possible subsequent handover delay is reduced and interactive communications (e.g. VoIP) are less affected by the authentication delay.

Proactive pre-authentication using MIHS is not a novel research topic and the authors are well aware of this. In [26], a MIH information service is queried to discover surrounding access networks and to proactively initiate secure SIP registration with

candidate SIP registrars. Similarly, [27] reviews network topology description and discovery mechanisms for proactive handover. However, none of those approaches consider the full MIHS architectural framework. As a consequence, we propose hereafter an integrated approach using off-the-shelf pre-authentication mechanisms together with OpenMIH. The resulting architecture allows to proactively control pre-authentication using different MIH services such as MIIS for topology discovery and MIES for timely-significant indication of link change.

5.1 Scenario Outline

The scenario that we consider is depicted in Figure 3: a mobile node is under mobility in a wireless environment made available by a set of wireless network access providers. Due to the current mobile node applications requirements in terms of security, data integrity and confidentiality, handover policies are set to only select PoAs that feature robust wireless security. In addition, user preferences favor the choice of Wi-Fi access network over WiMaX or 3G for power consumption reasons. Part of its subscription, the mobile node benefits from an unlimited access to a WPA wireless access network operated in the area and was accordingly provisioned with appropriate credentials for authentication.

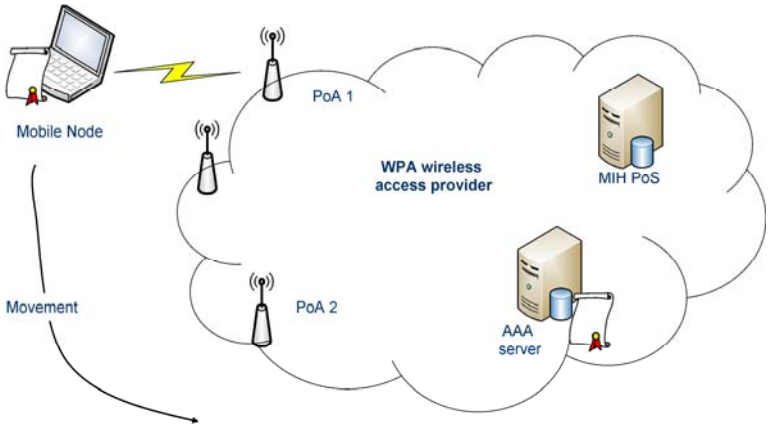


Fig. 3. Proactive pre-authentication scenario outline

Without MIHS, candidate PoAs may be detected by scanning (passive or active) but are discovered only when the mobile node enters the candidate PoA's wireless coverage. To extend the range of the topology discovery and to anticipate handover decisions and operations, we use network topology information provided by a MIH PoS and filter the results according to the mobile node's location and user preferences. The information is described in a rich information format and stored in a database co-located with the MIH PoS. It includes information such as: network operators, PoAs and QoS information.

5.2 Proactive pre-Authentication Execution

The software components involved in the abovementioned scenario are illustrated in Figure 4. As it is a mobile-controlled handover, we only depict the mobile node's software stack:

- *WPA_supplicant* is part of the hostapd software suite [28] that allows setting up Wi-Fi Protected Access (WPA) networks. As such, it comes as two complementary software packages: hostapd for securing a Wi-Fi PoA and wpa_supplicant for the client side. They permit to configure a large set of security suites (TKIP, CCMP) and authentication methods (e.g. EAP-TLS / PEAPv2/ EAP-SIM) and allow to set up secure associations with most of Wi-Fi drivers supported by the Linux operating system (through the Linux wireless APIs: wireless extensions and nl80211 [29]).
- *Pre-authentication manager* is responsible for network selection, proactive pre-authentication control and homogeneous handover triggering. It is a MIHU for OpenMIH and communicates with the MIHF with IPC (as detailed in section 4). It also uses wpa_supplicant control interface for configuring and controlling (pre-)authentication via a UNIX socket.
- *MIH Wifi driver adapter* is a link adapter as defined in section 4. Its role is to implement the media-specific Wi-Fi amendments for interoperability with MIHS. In our case, the mostly used primitive is the predictive `Link_going_down` event that indicates the forecasted link loss. For repeatability, this event is generated using a Wi-Fi signal simulated from a two-ray propagation model [30].

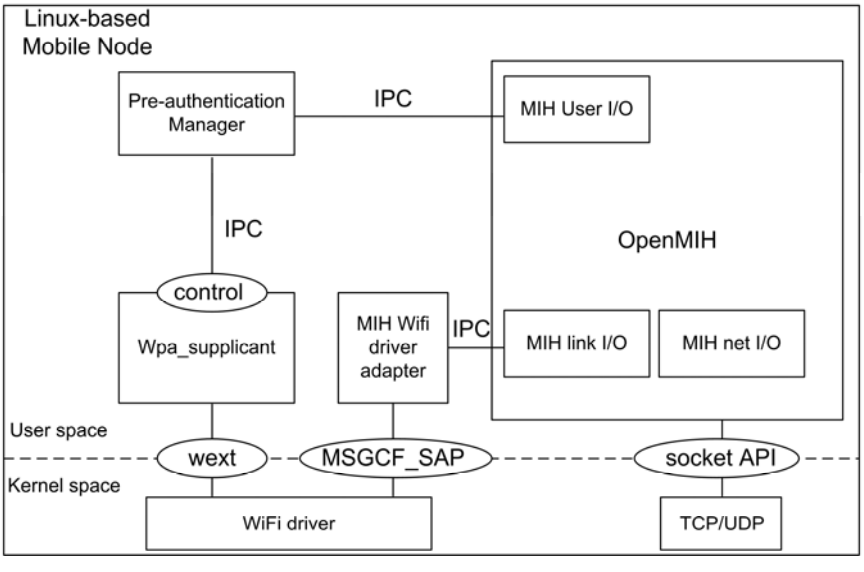


Fig. 4. Integrated software architecture of a Linux-based Mobile Node for proactive pre-authentication using OpenMIH

The mobile node's integrated architecture has been tested for the scenario presented in section 5.1. The corresponding sequence diagram is depicted in Figure 5.

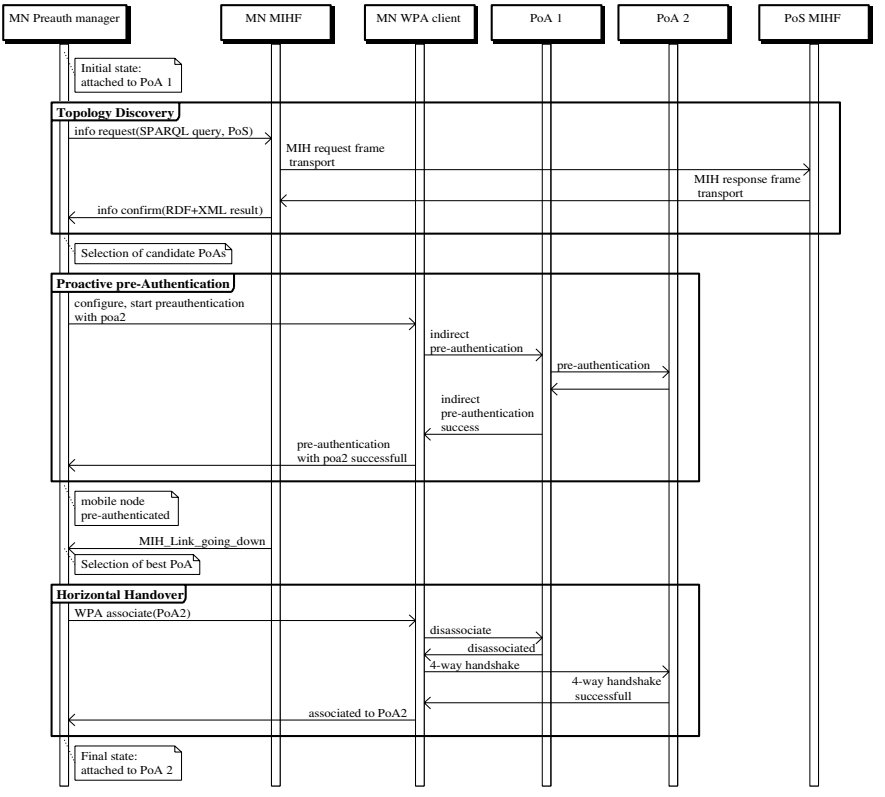


Fig. 5. Sequence diagram for mobile-controlled proactive pre-authentication using OpenMIH

In addition to the Mobile Node (MN) components described above, it involves two PoAs and a MIH PoS. In our scenario, proactive pre-authentication involves three subsequent steps:

- *Topology discovery*: initially, we assume that the MN has successfully authenticated with PoA1 using EAP-TLS authentication method and is associated. During topology discovery, we involve a MIH PoS that holds a detailed description of the network topology, including the PoA parameters (e.g. frequency, WPA cipher suites, authentication method). Several proposals exist for discovering a PoS but in our scenario, it is legitimate to assume that the MIH PoS is statically provisioned to the MN MIHF by its provider and that no additional discovery is needed. The MN pre-authentication manager is able to initiate a MIH information request and to retrieve the results. The query uses the SPARQL query language and contains information on the current mobile's node location and its user preferences on security, which allows an accurate filtering of the results. The RDF/XML query result gives the necessary information to the pre-authentication manager that processes it to extract the relevant attributes.
- *Proactive pre-authentication*: during this phase, proactive pre-authentication is initiated with all candidate PoAs (i.e., the PoAs the mobile node identified as possible

next attachment points based on its location, direction and security requirements) by formatting the retrieved PoA information and sending the appropriate IPC to MN WPA client. In the sequence diagram, one can notice that pre-authentication is only depicted for PoA2. As the MN has only one Wi-Fi interface, pre-authentication with PoA2 is indirect over the current association with PoA1. Upon successful pre-authentication, PoA2 and MN share transient keys that may be used for subsequent authentication.

- *Horizontal handover*: when the current link is degrading, the MN MIHF reports a `MIH_link_going_down` event to the MN pre-authentication manager that triggers the necessary actions to select the "best" PoAs that cover the area and that share transient keys from a previous successful pre-authentication. Then, the handover process takes place and consists in disassociating with PoA1 and in securely associating with PoA2. As transient keys are already shared between MN and PoA2, the authentication is reduced to the 4-way handshake.

6 Conclusion and Future Work

This paper presents OpenMIH, an opensource implementation of MIHS and an integrated architecture for proactive pre-authentication. We described the scope of the implementation, motivated its event-based architecture and detailed the various software components. We also showcased the OpenMIH implementation with an illustrative scenario for enhancing network selection and handover preparation in a secure wireless environment. We believe that experimental evaluation of MIHS is important and that is the reason why OpenMIH is publicly distributed with an open-source license. Therefore, we expect researchers, developers to use it, modify or extend it as soon as they abide by the license terms.

Our future work on OpenMIH includes different directions. Firstly, improving the conformance of the implementation with the standard: part of the MIHS standard, a normative Protocol Conformance Statement (PICS) proforma is provided (annex M) in order to assess the capabilities and options that are implemented by a particular implementation. Initially, OpenMIH releases will not detail the conformance with a PICS due to the lack of testing environment but it is expected to supply one in the subsequent releases to reflect the conformance level. Secondly, the application that is demonstrated in this paper is for horizontal handovers and only requires a restricted set of the MIH services. To go further, we expect to integrate various link adapters, comprising extensions to mesh-based networks, to specifically address richer scenarios involving vertical handovers between hybrid networks.

References

1. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6. IETF, RFC 3775 (2004)
2. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: Session Initiation Protocol. IETF, RFC 3261 (2002)
3. Moskowitz, R., Nikander, P., Jokela, P., Henderson, T.: Host identity protocol. IETF, RFC 5201 (2008)
4. Gustafsson, E., Jonsson, A.: Always best connected. IEEE Wireless Communications 10(1), 49–55 (2003)

5. IEEE 802.21 Working Group, http://ieee802.org/21
6. IEEE Std 802.21-2008, IEEE Standard for Local and Metropolitan Area Networks, Part 21: Media Independent Handover Services, IEEE (2009)
7. Lee, W., Kang, M., Lim, M.: Implementation of 802.21 for Seamless Handover Across Heterogeneous Networks. In: Ata, S., Hong, C.S. (eds.) APNOMS 2007. LNCS, vol. 4773, pp. 326–333. Springer, Heidelberg (2007)
8. Unified Link Layer API, http://ulla.sourceforge.net/
9. Piri, E., Pentikousis, K.: Towards a GNU/Linux IEEE 802.21 Implementation. In: IEEE International Conference on Communications, ICC 2009 (2009)
10. The ns-3 network simulator, http://www.nsnam.org
11. IEEE Std 802.11r-2008, IEEE Standard for Local and Metropolitan Area Networks, Part 11, Amendment 2: Fast Basic Service Set (BSS) Transition
12. IEEE Std 802.16e-2008, IEEE Standard for Local and Metropolitan Area Networks, Part 16, Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands
13. OpenMIH public website, http://openmih.sourceforge.net
14. Survey on asynchronous I/O methods, http://www.kegel.com/c10k.html
15. libevent, an event notification library, http://monkey.org/~provos/libevent
16. Stevens, R.: UNIX Network Programming, 2nd edn. Interprocess Communications, vol. 2. Prentice Hall, Englewood Cliffs (1999)
17. IEEE Std 802.11u-D6.0, IEEE Standard for Local and Metropolitan Area Networks, Part 11, Amendment 7: Interworking with External Networks
18. IEEE Std 802.16g-2007, IEEE Standard for Local and Metropolitan Area Networks, Part 16, Amendment 3: Management Plane Procedures and Services
19. Melia, T., Bajko, G., Das, S., Golmie, N., Zuniga, J.C.: IEEE 802.21 Mobility Services Framework Design (MSFD). IETF Internet-Draft (2009)
20. W3C Recommendation, Resource Description Framework (RDF), Concepts and Abstract Syntax, http://www.w3.org/TR/rdf-concepts
21. Survey of implementations supporting RDF and SPARQL querying, http://esw.w3.org/topic/SparqlImplementations
22. Redland RDF libraries, http://librdf.org
23. W3C Recommendation, SPARQL Query Language for RDF, http://www.w3.org/TR/rdf-sparql-query/
24. Griffith, D., Rouil, R., Golmie, N.: Performance Metrics for IEEE 802.21 Media Independent Handover (MIH) Signaling. In: Wireless Personal Communications. Springer, Netherlands (2008)
25. libyaml library, http://pyyaml.org/wiki/LibYAML
26. Silvana, G.P., Schulzrinne, H.: SIP and 802.21 for service mobility and Pro-active Authentication. In: 6th Annual Communication Networks and Services Research Conference, 2008, pp. 176–182 (2008)
27. Dutta, A., Madhani, S., Zhang, T.: Network Discovery Mechanisms for Fast-handoff. In: 3rd International Conference Broadband Communications, Networks and Systems, 2006, pp. 1–11 (2006)
28. hostapd software suite, http://hostap.epitest.fi/hostapd
29. Linux kernel wireless page, http://wireless.kernel.org
30. Barsocchi, P., Oligeri, G., Potorti, F.: Measurement-based frame error model for simulating outdoor Wi-Fi networks. IEEE Transactions on Wireless Communications 8(3), 1154–1158 (2008)

Bandwidth Sensitive Adaptation of Applications during MRM Controlled Multi-Radio Handover

Oliver Blume[1], Jens Gebert[1], Manuel Stein[1],
Dmitry Sivchenko[2], and Bangnan Xu[2]

[1] Alcatel-Lucent Deutschland AG, Bell Labs,
Lorenzstr. 10, 70435 Stuttgart, Germany
{oliver.blume,j.gebert,manuel.stein}@alcatel-lucent.de
[2] Deutsche Telekom / T-Systems,
Deutsche-Telekom-Allee 7, 64295 Darmstadt, Germany
Bangnan.Xu@t-systems.com, Dmitry.Sivchenko@telekom.de

Abstract. In heterogeneous radio access networks mobile terminals can dynamically change their radio access not only between access points but also between different radio access technologies (RATs). We present a network based Multi-Radio Management (MRM) for seamless control of inter-RAT mobility. Access Selection can be triggered by a change of radio channel quality, by the start of an application or by system load and handover is executed by enhanced MobileIPv6. Dynamic adaptation of the IMS services, e.g. adaptation of IPTV to the available bandwidth, is realized by triggering additional mid-call SIP signaling between communicating parties so that Quality of Experience (QoE) can be significantly improved. The described MRM and dynamic adaptation of IMS services are validated by a prototypical implementation in an integrated demonstrator.

Keywords: Multi-radio handover, vertical handover, MRM, MRRM, radio access selection, ASF, IMS, codec adaptation, SIP re-invite, SIP codec adaptation.

1 Introduction

Today, many different radio access technologies (RATs) such as GSM [1], UMTS [2], CDMA2000 [3], WLAN [4] or WiMAX [5] coexist in parallel—quite often in an overlaying deployment by the same operator. Such operators need network solutions that provide their subscribers with ubiquitous mobile services in overlay cells, hotspots, indoor-coverage, and added cells with future wireless technologies. Inter-RAT mobility between 3GPP technologies (GSM, UMTS, HSPA, LTE) and non-3GPP technologies (CDMA2000, WiMAX, WLAN) is currently being standardized in the 3GPP evolved packet system (EPS) [6]. But the specification is still missing a network based decision functions for inter-RAT access selection although some related work has been initiated in 3GPP in the scope of the Access Network Discovery and Selection Function (ANDSF)[1] [6]. Furthermore, the change of

[1] ANDSF supports terminal based multi-radio access selection by network based policies.

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 26–37, 2010.

available QoS (e.g. the supported data rate) during handover is not communicated to the application layer. In this paper we describe a multi-radio management (MRM) function that monitors the radio link quality of the serving cell and of the candidate cells, anticipates the change of available bandwidth caused by a planned handover and triggers the IMS application function to adapt the running SIP services, e.g. to change the codec of a video stream.

A major issue for such inter-RAT access selection and for cross-layer optimization of the QoS is that different RATs use different measurement values and metrics to quantify the radio channel quality. The envisioned interworking thus requires abstraction and adaptation functionality between radio layers and MRM to map the specific link quality values to a generic scale of values that can be compared to application QoS values. Some standardization bodies are working on general interworking solutions, such as the IEEE Media independent Handover (MIH) framework [7]), but they do not provide solutions to metrics for inter-RAT access selection. This paper presents an integrated solution comprising the MRM concept [8][9] developed by Alcatel-Lucent Bell Labs and the IMS enhancements [10][11] developed by Deutsche Telekom / T-Systems. This work has been undertaken in the framework of cooperative projects, such the German Federal Ministry of Research and Education's (BMBF) project "Scalable, Efficient and Flexible Networks" (ScaleNet) [12] and the European Union's (EU) project "Ambient Networks" [13].

2 Multi-Radio Management

In a heterogeneous wireless environment mobile terminals can dynamically change their radio access not only between access points but also between different radio access technologies (RATs). For a change of the radio access, i.e. for an inter-RAT handover, the mobile terminal (1) has to measure the radio link quality of the serving radio link and of candidate radio links in other technologies and (2) to take access selection decision to figure out if and when one of the candidate cells offers a better service than the currently serving cell. Due to battery constraints of the terminals it is not possible to continuously scan over all radio channels on all radio interfaces. Instead, a multi-radio capable functionality with knowledge of the terminal's position and of the network topology and status shall advertise nearby candidate cells.

Such a coordinated operation of several RATs requires the introduction of an overarching and generic resource and mobility management residing above the legacy Radio Resource Management (RRM) and Mobility Management (MM) of the individual technologies. This new entity is called Multi-Radio Management[2] (MRM) [8]. MRM functions are typically distributed over the core network, the access networks and the mobile terminals. To take full benefit of MRM and to allow operator control over the load distribution, it is preferable to deploy the access selection function in the network [8].

The main functions of MRM are described in more details in the following sections.

[2] MRM is sometimes also called Multi-RRM (MRRM), Joint RRM (JRRM), Heterogeneous RRM (HRRM) or Common RRM (CRRM).

2.1 Abstraction and Adaptation Layer

The mechanisms and procedures for link control strongly differ between radio access technologies, i.e. MRM would have to operate different access selection algorithms and different handover mechanisms for each pair of RATs. This requires specification and interfaces involving multiple standardization bodies and large implementation effort.

Therefore, an abstraction and adaptation layer (AAL) is defined between MRM and the radio interfaces, hiding the RAT-specific properties from the generic MRM (Fig. 1). The main functions of this layer are the translation of generic MRM procedures to RAT-specific procedures and the mapping of RAT-specific values to generic values and vice versa. For example, a generic link setup request of MRM may be mapped for IEEE 802.11 WLAN into a sequence of Mlme.Join, Mlme.Authenticate and Mlme.Associate primitives as specified by the WLAN protocol [4]. More examples for the translation process are given in [8].

The advantage of these abstraction and adaptation function becomes particularly visible when new radio technologies are integrated into existing systems. In this case, the MRM as well as the AAL for existing RATs remain unchanged, while only the adaptation and abstraction functions needs to be implemented for the new RAT.

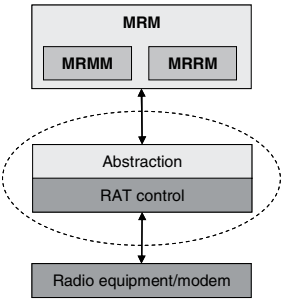


Fig. 1. Abstraction from RAT specific to generic values and commands

2.2 Multi-Radio Measurements

The radio link quality is expressed in different RATs as a radio signal strength (in dBm or as relative RSSI values, e.g. in 802.11 WLAN), as a signal-to-noise value (SNR, SNIR, given in dB), as bit error rate (e.g. in 10^{-4}) or as relative channel quality indicator CQI (e.g. in 3GPP HSDPA). These link quality values are not directly comparable between each other, nor to the QoS requirements of the running service. The abstraction layer thus recalculates these values according to each RATs specifications into an available peek data rate at a given residual bit error rate. Furthermore, if the RAT supports QoS guarantees, it also calculates the granted minimum data rate and the transmission delay [8].

MRM configures generic link quality measurement requests at the interface to AAL to receive periodic and event-based link quality measurements. Candidate measurement requests are based on the advertisement of surrounding cells. For

moving users, detection of entering or leaving hotspots with broadband coverage has to be performed fast and efficiently to enable well-informed MRM decisions.

In the same abstracted way, MRM on network side collects load information to assess the availability status of the cell resources.

2.3 Access Selection

Radio access selection denotes the process of choosing for a terminal (at a given location and running a given service) the most appropriate access technology and point of attachment (cell or access point) within a heterogeneous network. However, inter-technology handover is not always reasonable. E.g., real time services may not be well supported by a best effort WLAN hotspot or fast moving mobile terminals may reside within a hotspot for too short an amount of time. Therefore, access selection algorithms need to be configured in terms of operator and user criteria [13].

Access (re)selection decisions are taken proactively based on the abstracted link quality measurements, in order to seamlessly finalize the handover execution before a fading link breaks. This enables always-best connectivity for mobile users.

Next to the provisioning of best connectivity to the user, access selection also offers operators the potential of optimizing network usage and revenue. Obviously, inefficient service distribution between the different access systems may lead to overload on some access systems, while resources in alternative access systems are still available. Moreover, depending on the link performance and the service type, the resource costs of different access technologies differ, leading to a potential for overall capacity increase.

In the presented implementation, MRM applies a decision algorithm with a weighted metric regarding abstracted link quality, application QoS requirements, and system load. The Access Selection Function (ASF) can either be implemented distributed over the access networks or as a centralized service on a Heterogeneous Access Management (HAM) server in the operator's core network [8].

2.4 Mobility Management

Furthermore, MRM comprises a mobility management, which coordinates the time sequence of build-up and release of the radio connections during handover execution. Depending on the capabilities of the mobile terminal different handover protocols and handover sequences can be used [9]. In this article, we assume use of Mobile IP protocol IPv6 [14] and that the terminal is capable of connecting the target radio link before releasing the source link, so that a seamless make-before-break handover can be performed.

3 IP Multimedia Subsystem

The IP Multimedia Subsystem (IMS) [15] is an architectural framework in 3GPP EPS for delivering Internet Protocol (IP) multimedia services independently of the type of wireless access or wired access (fixed mobile convergence, FMC).

The IP Multimedia Subsystem (IMS) is used to forward the complete Session Initiation Protocol (SIP) [16] signaling used in the IMS for session management. A

number of Call Session Control Functions (CSCF) are introduced to establish a multimedia session between subscribers and to prepare delivery of the demanded services according to the session characteristics required by users. Some of CSCFs have interfaces to the Home Subscriber Server (HSS) where the complete information about particular subscribers is stored, like their profiles, policies, subscriptions, preferences, etc.

Three types of CSCFs are defined:

- Proxy-CSCF (P-CSCF) is the first point of contact for the IMS users. The main goals of the P-CSCF are the guarantee of signaling messages between the network and subscriber and resource allocation for media flows by the interaction with Resource and Admission Control.
- Serving-CSCF (S-CSCF) is the main control entity within the IMS. It processes registrations from subscribers and stores their current location, is responsible for subscriber authentication and call management. Subscriber policies stored in the HSS control the operations performed by the S-CSCF for a particular subscriber.
- Interrogating-CSCF (I-CSCF) queries the HSS to find out the appropriate S-CSCF for the subscriber. It can also be used to hide operator's network topology from other networks.

4 Bandwidth Adaptation of Applications

MRM monitors serving and candidate radio link qualities with respect to the requested QoS of the running application. When MRM decides on a handover to provide best possible service the provided data rate may change. MRM as described in [8] does not interact with the running applications. Further mechanisms are required to adapt the service to the available bandwidth. For example, when the mobile terminal enters a hot spot with high data rate the resolution of a video stream could be improved from VGA to HDTV. In case the bandwidth reduces, e.g. when leaving a hotspot, the high data rate will rapidly fill the transmission queue of the target RAT and packets will be dropped, either by policing or simply by buffer overflow. Both will cause artifacts or freezing of a video stream as shown in Fig. 6b. The disruption of the video stream reduces the QoE for users dramatically as it is not possible to continuously follow the video content.

Different mechanisms on application layer will be briefly discussed for adaptation of the data rate.

4.1 UDP Applications

The User Data Protocol (UDP) [17] is a best-effort protocol without flow control, accepting incoming data as-is. Often the Real Time Transport Protocol (RTP) [18] is run on top of UDP. Video streaming with a data rate determined by the video source is a typical example for a service running over RTP/UDP/IP. A higher available data rate on the link will not be used, a lower data rate on the link will lead to vey low quality[3].

[3] If the terminal runs some kind of application manager (e.g. the user interface of a PDA) data rate monitoring may be used to stop the application if the data rate drops below a minimum.

4.2 TCP Applications

TCP [19] is a transport protocol providing reliable transmissions and which adapts the data rate according to the round trip time between communicating peers. TCP quickly reduces the data rate in case of congestion and slowly ramps-up to a higher data rate if served well. This efficiently adapts the data rate of applications that can send data as fast as the queue is emptied, e.g. non-realtime services like file downloads using File Transfer Protocol (FTP) [20]. However, the basic TCP does not take benefit from anticipated data rate changes during MRM handover [4] and the ramping is not suitable for applications with a fixed packet rate, like real-time video streaming.

4.3 IMS/SIP Applications

IMS/SIP applications also use UDP or TCP transport. But on top of the transport layer, the data rate of the applications is negotiated between the communicating peers (e.g. between a terminal and a video server) during session establishment using SIP INVITE messages. Within these messages a list of supported codecs is exchanged. SIP RE-INVITE messages can be used to adapt the codec at any time during the running service. In IMS, the IMS Application Function (AF) is introduced to be located on a CSCF and that acts as a SIP proxy mapping a codec to the required QoS parameters (e.g. bit rate, BER) on the IP layer. Doing so, AF is able to change the codec depending on the IP resources available for user on the transport plane.

Interworking of MRM and IMS AF opens the possibility to use the knowledge of abstracted link performance not only for MRM access selection but also for adaptation of the codec and of codec parameters of running multimedia sessions. During start of a SIP session the IMS AF registers at MRM for QoS status information, supplied by AccessFlow.Indications with the actual user plane data rate. When the data rate changes, e.g. at an MRM induced handover event, the IMS AF receives the newly available data rate from MRM. AF then enforces codec adaptation by sending SIP RE-INVITE messages with the new codec to the terminal and to the media server (Fig. 2).

For the pro-active handover execution two cases have to be distinguished:

- When the AccessFlow.Status.Indication of the target RAT shows a higher data rate the current codec shall be used until the handover is executed. After the data plane has been switched (i.e. after MIPv6 Binding Update) the AF enforces the use of a larger codec to provide better QoE to the user utilizing the increased data rate.
- If the candidate radio link offers lower bandwidth than the current radio link (e.g. for a fading link when leaving coverage of a hotspot) the change to a codec requiring a lower bit rate must happen before the switching of the data plane to the new radio link. Otherwise the data rate will rapidly fill the transmission queue and buffer overflow or policing of RRM will lead to dropping of packets and bad user experience. Instead, MRM must send an AccessFlowStatus.Indication to the AF before executing the handover. Only after the codec has been re-negotiated MRM can trigger the MIPv6 binding update.

[4] Like for UDP transport, an application manager can be used to terminate the application if the data rate drops below a minimum, or the remaining download time increases unacceptably.

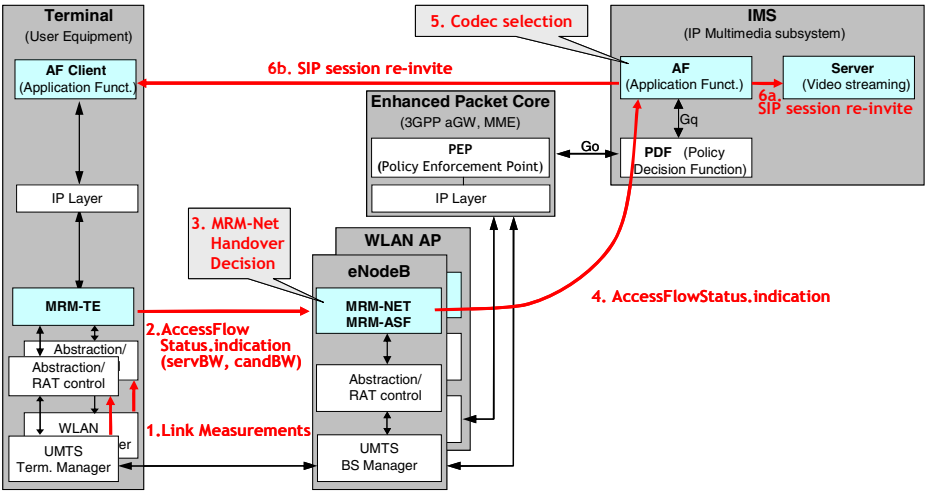


Fig. 2. Signaling of MRM and IMS for bandwidth adaptation to radio link bandwidth

5 Demonstrator

In order to validate the MRM and IMS enhancement concept, a demonstrator [22] has been set up comprising two different radio access networks and a dual-radio mobile terminal.

5.1 Demonstrator Set-Up

The MRM demonstrator [8,9,22] consists of a 3GPP UMTS/HSDPA overlay cell, two small IEEE WLAN hotspots and a dual-radio mobile terminal. The integrated MRM & IMS demonstrator extends this with the extended IMS functionality based on the IMS implementation [21]. On the network side an IPv6 application server and an IPv4 IMS server have been integrated (Fig. 3). The demonstrator supports IPv6 mobility for handover during ongoing services of different QoS classes, i.e. FTP based file transfer, Web browsing via Hypertext Transfer Protocol (HTTP) [23], video streaming via UDP and RTP controlled manually or using SIP/IMS.

Generic MRM instances are implemented in the terminal, the core network, and the access networks of each RAT. Between the MRM instances an interface has been specified and implemented based on the Diameter [24] protocol. For the cross-layer interaction between MRM and MIPv6 in the terminal the standard interface to the IP kernel functions is used. The interface between MRM and the abstraction function has been implemented for an UMTS base station (Alcatel-Lucent Evolium NodeB) and for an WLAN 802.11a-based access point (Signalion Sorbas AP). Real radio signal strength measurements are acquired. The movement of the dual-radio terminal is emulated by changing the link performance with a radio frequency (RF) attenuator at the WLAN antenna. The network based MRM Access Selection Function (ASF) thus has access to generic resource status information from MRM modules communicating with UMTS and WLAN interfaces in the terminal and in the access networks. It

triggers handovers according to the requested QoS level, the currently available data rate for both access interfaces of the terminal, and the handover policies. MIPv6 handover execution is caused by changing the interface preference in the terminal.

Most parts of the demonstrator are implemented on LINUX platform, but the UMTS control function of the HSDPA test mobile and the IPv4 SIP client run on WINDOWS OS with IPv4 interfaces. Therefore, the User Terminal comprises a network of three computers and compatibility to the IPv6 demonstrator has been achieved by IP6-in-IP4 tunneling mechanisms.

The MRM-demonstrator setup with a distributed MRM deployment is shown in Fig. 3.

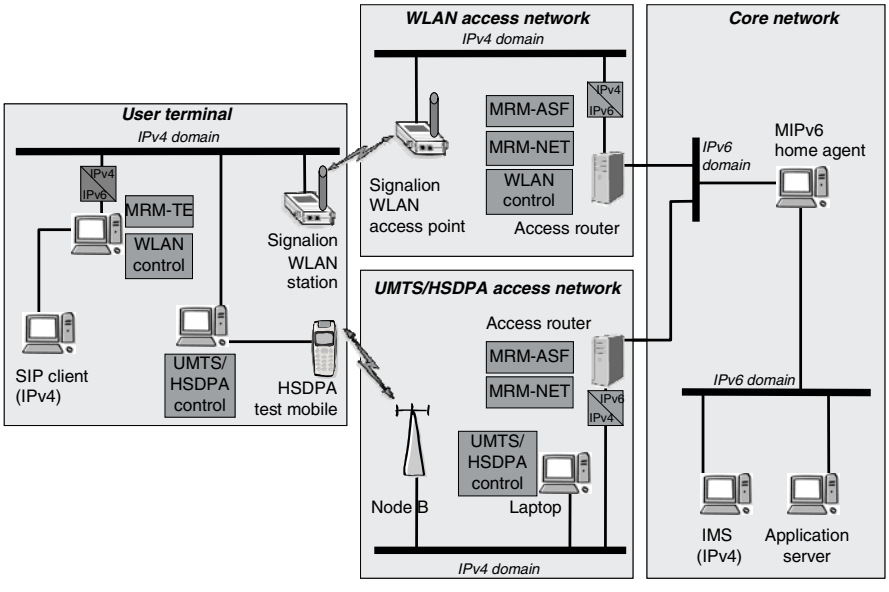


Fig. 3. Demonstrator Setup

The user terminal implements a standard IMS client to be able to initiate and to maintain video streaming services controlled by the IMS. The IMS server [10,11] has been extended with an IMS-MRM Proxy function that communicates with IMS AF deployed on the P-CSCF using standardized Gq' interface. On the other side, it implements the proprietary MRM interface so that signaling messages regarding QoS requests can be translated to MRM signaling for management of resources on the transport plane. The IMS-MRM Proxy function allows the IMS controlled session management to request for an IMS application a minimum and maximum usable QoS level on the access. It receives data rate reports by MRM AccessFlow-Status.Indications and executes dynamic application codec selection when the measurement value exceeds this range.

Fig. 4 shows the detailed architecture of the integrated MRM & IMS demonstrator.

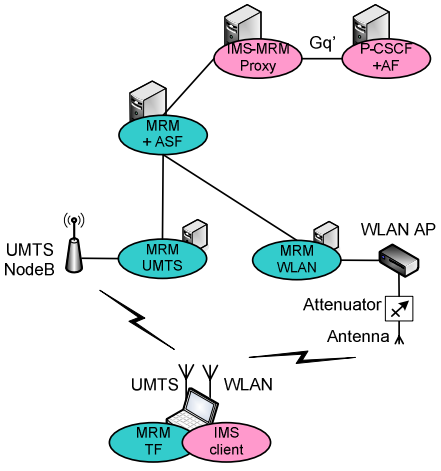


Fig. 4. Architecture of the integrated MRM & IMS demonstrator

5.2 Demonstrator Results

The feasibility of the MRM concept and the scalability by MRM distribution were verified successfully. The distributed MRM instances on network side (MRM-NET) trigger handover decisions in a central or co-located decision function (MRM-ASF) based on abstracted radio link measurements, application type, operator preferences and cell loads. MRM instructs the user terminal to perform a MIPv6 handover between the two heterogeneous RATs. The trigger levels, the decision algorithm, and the simultaneous availability of both radio interfaces during handover (make-before-break versus break-before-make) can be configured. The resulting handover performance is determined by user-perceived service interruption and by measurements of packet loss and transmission time.

The data rate of an FTP file download over UMTS/HSDPA is limited in the demonstrator to 300kBit/sec due to the 80 msec delay on the UMTS uplink. During the handover from HSDPA to WLAN, TCP ramps up the download rate to 3.5MBit/sec and in the other handover direction it successfully prevents congestion by returning to 300kBit/sec. For UDP video streaming with a data rate below 1MBit/sec both RATs support the data rate and MRM performs pro-active handovers seamlessly in both directions, adaptation by IMS AF is not required in this case.

MRM decided handovers have also been successfully performed during video streaming service controlled by IMS/SIP. Fig. 5 shows the reduction of WLAN signal strength caused by a stepwise increase of the attenuator. Handover is performed at 20% relative signal strength where the abstraction layer calculates that the currently used WLAN data rate drops below the data rate estimated from the measurements of the UMTS candidate link (1000 kBit/sec in Fig. 5). MRM sends an AccessFlow-Status.Indication to the MRM-IMS Proxy with information about a newly available data rate for the terminal of 300 kbit/s. MRM-IMS Proxy informs the AF via the Gq' interface which then initiates the adaptation of the codec bit rate parameter for the established video session. After the UMTS target link is established in a make-before-break

handover, the data is then transported via the UMTS radio link. Due to limited computing power of the IMS server (implemented on a desk top PC) the re-coding of the video stream leads to a short interruption of the data stream at the source which is sometimes perceivable to the watchful eye. Fig. 6 shows a screenshot of the video quality over WLAN before the handover (Fig. 6a) and the reduced quality after adaptation of the service to the data rate over UMTS/HSPA (Fig. 6c). Please note that without the codec adaptation, the transmission buffer of the NodeB would be quickly filled and about 90% of the packets would be dropped. The video and sound quality would be completely inacceptable without such a codec adaptation (Fig. 6b).

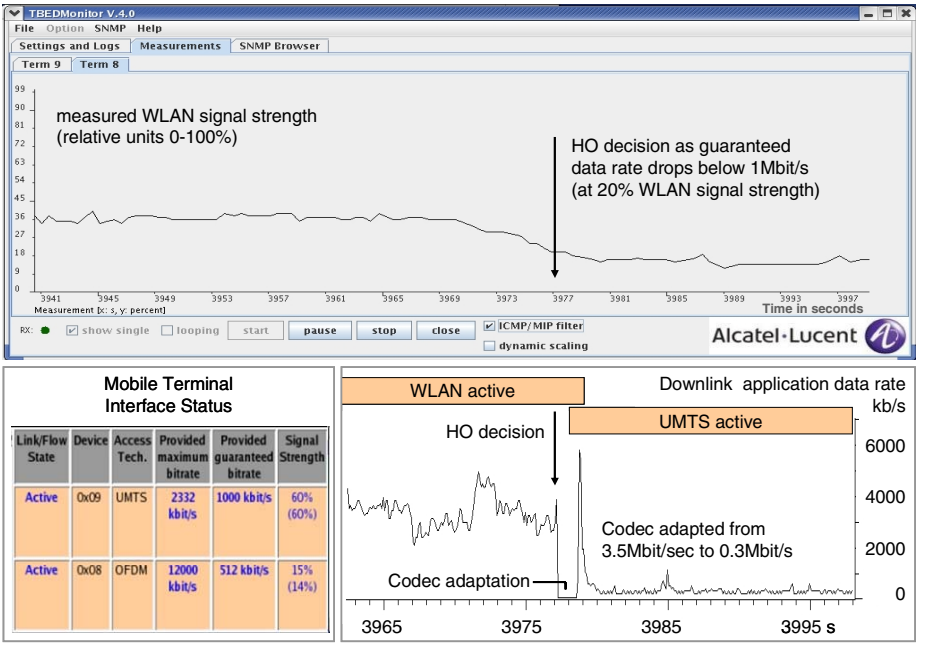


Fig. 5. Signal Strength and Video Streaming Downlink Data Rate during handover to a radio link with lower data rate capability

Fig. 6. By adaptation of IMS codec before Handover streaming can continue with reduced resolution (screen shot of video (a) before handover, (b) after handover without adaptation and (c) after handover with MRM/IMS codec adaptation)

5 Conclusion

Fourth generation wireless networks will probably consist of multiple, heterogeneous radio technologies, requiring intelligent interworking solutions. The multi-radio management (MRM) concept is one necessary step towards a pervasive and effective integration of current and future access technologies. MRM handles the differences between heterogeneous access technologies in a unified way by abstraction from RAT-specific parameters and adaptation to RAT-specific functionality in an adaptation and abstraction layer (AAL). The proposed general approach leads to a significant reduction of standardization and implementation efforts compared to bilateral interworking solutions between each pair of radio access technologies.

The MRM functions and architecture were discussed, the key functionality of MRM is a network-based, pro-active radio access selection mechanism that considers radio link performance, resource usage, and user and operator preferences. For seamless inter-technology handovers, MRM synchronizes IP mobility protocols with link and session layer procedures. This approach enables inter-RAT access selection and common resource and mobility management for all RATs, offering the potential to optimize network usage.

Even though MRM performs handovers seamlessly, the data rate may change in case of inter-RAT handover and this can spoils high user QoE. By interworking of MRM with the IP Multimedia Subsystem (IMS) the MRM information about the actual link performance can be utilized to match the available data rate by adapting the codec with a SIP RE-INVITE, either before or after handover execution.

The feasibility of the MRM concept and its integration with IMS have been realized and validated in an MRM/IMS demonstrator offering seamless IP-mobility between a cellular UMTS/HSDPA network and a WLAN hotspot during ongoing multi-media sessions. MRM measurements of radio link QoS and handover triggers are leveraged in the IMS for pro-active SIP codec adaptations. Nearly seamless adaptation of the quality of a video stream has been demonstrated for handover in both directions.

Based on these results the proposed MRM/IMS integration is a promising solution for future 3GPP enhancements of the EPS architecture, enabling added-value services and providing enhanced QoE in fourth generation wireless networks.

Acknowledgement

We gratefully appreciate the contributions of Bernhard Hahn, Dirk Hofmann, Thomas Klotsche, Achim Reichelt, Edgar Kühn and Rolf Sigle. This work has been partially funded by BMBF within the ScaleNet frame work.

References

1. Global System for Mobile Communications (GSM), `http://www.gsmworld.com/index.htm`
2. Universal Mobile Telecommunications System (UMTS), `http://www.3gpp.org/`

3. Code division multiple access 2000 (CDMA2000), http://www.3gpp2.org/
4. Wireless Local Area Network (WLAN), http://standards.ieee.org/getieee802/802.11.html
5. Worldwide Interoperability for Microwave Access (WiMAX), http://www.wimaxforum.org
6. Architecture Enhancements for Non-3GPP Accesses (Release 8), Technical Specification 3GPP TS 23.402 v8.2.0 (June 2008), http://www.3gpp.org
7. Media Independent Handover Services (MIH), IEEE 802.21/D8.1 (February 2008)
8. Sigle, R., Blume, O., Ewe, L., Wajda, W.: Multi-Radio Infrastructure for 4G. Bell Labs technical Journal 13(4), 257–276 (2009), http://www.interscience.wiley.com
9. Technologien für heterogene Zugangsnetze, Alcatel-Lucent project report in BMBF framework ScaleNet, Förderkennzeichen 01BU564 (2005-2008), http://tiborder.gbv.de/psi/
10. Sivchenko, D., Hahn, B., Xu, B., Rakocevic, V., Habermann, J.: Prototypical Realisation of IMS based QoS Concept with Mobility Support for FMC Access Networks, Mobilfunktagung, May 2008, vol. 13 (2008), http://www.vde-verlag.de/data/prcd.php?docid=453104013
11. Fixed, Mobile & Wireless IP-optimiertes konvergentes Zugangsnetz der nächsten Generation, Deutsche Telekom project report in BMBF ScaleNet framework, Förderkennzeichen 01BU561 (2005-2008), http://tiborder.gbv.de/psi/
12. Scalable, efficient and flexible next generation converged mobile, wireless and fixed access networks (ScaleNet). BMBF, (2005-2009), http://www.scalenet.de/index.htm
13. Tang, H., Gebert, J. (eds.): Multi-Access System Design and Specification, EU FP6 Ambient Networks II, D15-C.2 (December 2007), http://www.ambient-networks.org/deliverables.html
14. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6., RFC 3775, IETF (2004)
15. IP Multimedia Subsystem (IMS), Stage 2 (Release 8). Technical Specification 3GPP TS 23.228 V.8.7.0, 3GPP (December 2008), http://www.3gpp.org/ftp/Specs/html-info/23402.htm
16. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol, RFC 3261. IEEE, Los Alamitos (2002)
17. Postel, J.: User Datagram Protocol, RFC 768, IETF (August 1980)
18. Schulzrinne, H., Casner, S.H., Frederick, R., Jacobson, V.: RTP: A Transport Protocol for Real-Time Applications, RFC 3550, IETF (July 2003)
19. Postel, J.: Transmission Control Protocol, RFC-793 (September 1981)
20. Postel, J., Reynolds, J.: File Transfer Protocol (FTP). RFC 959 (October 1985)
21. OpenIMS playground, http://www.openimscore.org
22. Demonstrator presentation at BMBF Status Meeting 2008, Freiburg, June 18-19 (2008)
23. Fielding, R., Gettys, J., Mogul, J., Frystyk, J., Masinter, L., Leach, L., Berners-Lee, T.: Hypertext Transfer Protocol – HTTP/1.1, RFC 2616 (June 1999)
24. Calhoun, P.: Loughney, J. Guttman, E., Zorn, G., Arkko, J.: Diameter Base Protocol, RFC 3588 (September 2003)

Session 2:
Context and Connection Management

An Autonomic Connection Management Mechanism on Mobile Terminals*

Xiuli Zheng, Yuhong Li, Weiqi Hu, and Xiubin Zhuang

State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications,
Xitucheng Road, 10, 100876 Beijing, China
zhengxl1008@gmail.com, hoyli@bupt.edu.cn,
hu_weiqi@tom.com, zhuangxiubin@sina.com

Abstract. This paper proposes an autonomic connection management mechanism for multi-homed mobile terminals. The knowledge repository and the case-based reasoning technique are used to enhance the autonomicity of the connection management. The multi-criteria handoff decision is the core of the mechanism. Analytic Hierarchy Process (AHP) and Simple Additive Weighting (SAW) are combined to make the handoff decision. Simulation results and performance analysis show that the proposed mechanism works well in the heterogeneous wireless access network environment.

Keywords: Vertical handoff, connection management, autonomicity.

1 Introduction

Multi-homed terminals, which have more than one network interface or global address, can have several parallel communication paths simultaneously through attaching to one or more access networks. In heterogeneous wireless and mobile environment, the multi-connection scenario [1] puts forward great challenges to the connection management.

In the multi-connection scenario, the connection management is responsible for selecting the most suitable network for each application's connection and achieving effective use of the integrated networks resources. In heterogeneous wireless and mobile environment, the seamless vertical handoff for each connection needs to be considered, which is very important for both the effective use of the integrated network resources and the performance of the applications.

There are several advantages for performing connection management on mobile terminals (MTs). On the one side, the MT can gather various handoff related information. On the other side, it helps to decrease the complexity in networks and is beneficial for network's scalability related issues. However, since the miscellaneous factors have

* The work was supported by a grant from EU FP7 Project EFIPSANS (No, 215549) and Sino-Swedish Strategic Cooperative Programme on NGN (2008DFA12110).

[1] In this paper, a flow is a stream of packets from a source to a destination [1]; and a connection is regarded as a layer-3 logic path serving one flow of a particular application/service.

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 41–48, 2010.

to be handled, MTs may spend extra processing time and memory for performing connection management.

To simplify the connection management and expedite the handoff decision, autonomicity [2] is introduced in the connection management mechanism in the MTs.

The rest of the paper is organized as follows. Section 2 gives an overview of related work in the area of mobility management. The basic principle of the autonomic connection management mechanism, along with a proposed handoff decision making algorithm based on AHP and SAW is described in section 3. In section 4, the performance of the proposed algorithm is analyzed according to the simulation results. Conclusion and future work are stated in section 5.

2 Related Work

Great efforts on vertical handoff related work have been made in recent years [3]-[11]. In general, they involved two categories of issues. One focuses on proposing certain handoff architectures for heterogeneous network environment, such as the USHA proposed in [3], the SIGMA put forward in [4], and the hierarchical mobility management architecture suggested in [5].

The other category focuses on suggesting some specific handover decision making algorithms or mechanisms, such as work in [6]-[11]. Among them, some traditional vertical handoff algorithms considered only the RSS or the data rate as the key handoff trigger event, such as [6] and [7], whereas others put more efforts on studying the multi-criteria handoff decision algorithms, such as [9]-[10]. However, both the algorithms in [8] and [9] are just suitable for application or service granularity, which are inadequate to handle finer granularity handoff decision, such as the connection-based handoff decision.

Several works have tried to implement intelligence of the proposed algorithm, such as [10] and [11]. In [10], the adaptive interface activating method adjusted the interface activating interval only according to the distance between the MT and the base station. In [11], pattern recognition was used to estimate the user's position, and the handoff decision was based on the obtained information. Both these algorithms have introduced intelligence to some extent, but neither of them really made decision based on multiple criteria.

Compared with the above algorithms, the proposed autonomic connection management mechanism in our paper has the following features: (1) AHP and SAW are combined to handle multi-criteria vertical handoff decision. (2) Furthermore, it is designed to achieve connection based handoff decision, and can realize more accurate handoff decision for each service flow. (3) Knowledge repository with self-learning function is adopted, which could bring autonomicity into connection management.

3 Autonomic Connection Management

In general, the connection management involves the following operations:

(ⅰ) Making handoff decisions for connections;

(ⅱ) Influencing or controlling some behaviors of an MT and the corresponding network nodes, such as base stations (BSs) or access points (APs), during handoff;

(iii) Managing information of connections in an MT, stored in a CIL (Connection Information List). In our implementation, the CIL stores the identity and the corresponding information for all connections serving the applications in an MT. Each MT has a CIL, whose format is shown in Table 1.

Table 1. Format of a CIL

Connection Number	Connection Description
Con 1	(Status_Tag, Src.Uniq_ID, Dest.Uniq_ID, Flow_ID, Src.cur_IP, Dest.cur_IP, Service_Type)

In Table 1, each connection has one nonnegative integer as its identity, and can be identified by a five tuple: <Src.Uniq_ID, Dest.Uniq_ID, Flow_ID, Src.cur_IP, and Dest.cur_IP>. Here the Src.Uniq_ID and the Dest.Uniq_ID represent the unique identity for the source and the destination, respectively. Flow_ID is the identity of the flow served by the connection, which needs to be recognized by both the source and the destination. Src.cur_IP and Dest.cur_IP represent the current IP addresses used by the source and destination for the connection, respectively. Status_Tag with different values describes different status of connections. Service_Type represents the different service type. Information in the CIL needs to be updated or modified according to the changes of the environments.

3.1 Connection Management in MT

Connection management controlled by MTs is adopted in this paper. It is relatively easier for an MT to gather handoff related context information. Network status information could be measured by BSs and/or APs, and the results are sent to the MT. Other information, such as the application's requirement, user preference and device capability, can be collected by the MT itself. Using this mechanism, networks just assist the MT to do handoff decision and needs seldom changes on themselves.

3.2 Autonomic Connection Management

The connection management in our paper is an autonomic system, which has four steps forming a feedback loop as shown in Fig. 1. The system collects information from a variety of sources, which is analyzed to construct a case model of the evolving situation faced by the MT and its output by this model, i.e. certain a solution, is used as a basic

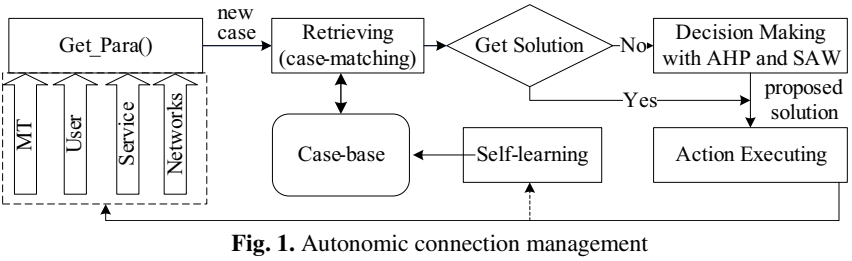


Fig. 1. Autonomic connection management

for intelligent decisions. The decisions are actuated through networks and MTs. The impact of decisions can then be collected to inform the next control cycle.

Step1 Context Collected by Get_Para()
Context information as follows needs to be collected for handoff trigger recognization, case matching in step 2 and multi-criteria handoff decision in step 3:

(ⅰ) *Network related factors*. The related factors of the networks where the MT roams to have to be collected, such as types of networks, availability of a network, limited available resources, their access mechanisms characteristics, etc.

(ⅱ) *Device related factors*. The capabilities of the MT include its battery life, processor speed, available interfaces. The MT's velocity is an important criterion.

(ⅲ) *Service requirement*. Wireless multimedia services can be classified into four service types, namely conversational service, streaming service, interactive services and background service [12]. Different types of services require various combinations of bandwidth, delay, jitter, reliability and cost.

(ⅳ) *User preference*. There are two criteria users are mainly concerned about, monetary cost and interface preference.

It is supposed here that the networks performance parameters can be acquired through the advertisement of the available access networks, or the MT can use data link layer probing or network layer probing. One result of Get_para() is a new case or problem description, which is used for the case matching in step 2.

Step2 Retrieving Similar Cases
Retrieving a case starts with a problem description and ends with whether a best matching case found or not. We adopt case based reasoning (CBR) techniques to implement the knowledge repository (KR). A case represents specific knowledge in a particular context. Case base is a cases library. Cases stored in the case base should be described clearly by "which service" using "which network" under "what conditions".

Table 2. Case description in CB

service type	velocity	network status	User preference	target network
Conversational,	x m/s	<Net1_para1,…,Net1_paraM>, ... <NetN_para1,…,NetN_paraM>	Pr_net1, ... Pr_netN	Net N

Case description is organized as Table 2. Each case has a vector description of service type, velocity, network status, user preference and target network.

Fuzzy matching is used to match the new case and cases stored in the CB. If a similar case is found, its solution can be directly reused to solve the current problem, going to step 4. If not, go to step 3 to generate a new solution.

Step3 Handoff Decision Making of A Multi-criteria Algorithm Based on AHP and SAW

A multi-criteria handoff decision making algorithm combining AHP and SAW will be described as follows.

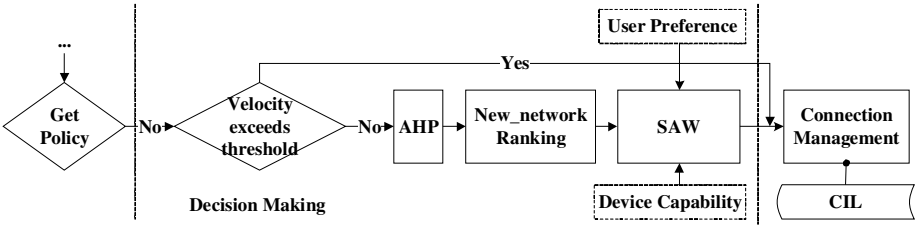


Fig. 2. Decision making with AHP and SAW

Step3.1 Velocity Judgment

As shown in Fig. 2, after all the necessary context information has been collected, the velocity of the MT is firstly analyzed to decide whether it is in the threshold scope. If it exceeds the threshold scope, just go to step 4. Nothing has to be done and CIL will be barely maintained. Otherwise, go to step 3.2.

Step3.2 Analytic Hierarchy Process (AHP) Based Network Ranking

AHP [13] is a well known and proven multi-criteria decision making approach to make the most appropriate choice among multiple alternatives based on some special goals. For AHP, all related factors are arranged in hierarchic structure, and paired comparisons in the same hierarchy are performed to generate priorities for criteria with respect to the predefined goal.

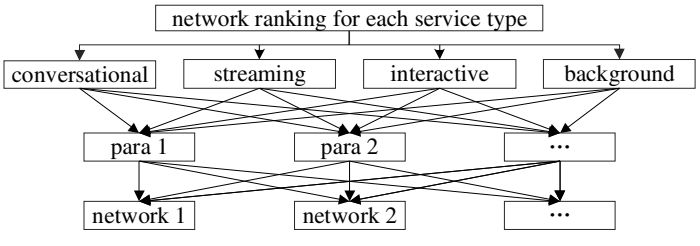


Fig. 3. Structure of the Analytic Hierarchy Process

Here AHP is used to get network ranking under the applications' requirements and the status of access networks. As shown in Fig. 3, the goal of "network ranking for each service type" locates in the first level. Four service types are in the second level. In the third level there are parameters that are considered with distinct importance by a factor in the upper level. Candidate networks reside in the fourth level.

Let's assume that parameters in the third level are bandwidth, delay, jitter, cost and reliability. Then we use the first four stages described in Section 3.2 of [8] to calculate

new network ranking value for each service type, which is calculated by the equation (1), similar to equation (13) in [8].

$$R_{i-j} = \sum_{k} p_{i-k} * p_{k-j} \tag{1}$$

In (1), i, j, k represents a service type, a candicate network, some parameter in the third level, respectively. p_{i-k} indicates the priority of parameter k among all parameters in the third level, for service type i. p_{k-j} indicates the priority of network j among all available networks in the fourth level, for parameter k. Both p_{i-k} and p_{k-j} can be gotten by equation (9) in [9]. R_{i-j} indicates the priority of network j among all networks, for service type i, and is always in the range of 0-1.

Step3.3Vertical Handoff Decision using SAW

After the network ranking for each service type is completed, handoff decision has to be made for each connection, which should take user preference and device capability into account. The priority of connection i in service type k W_{i-k} and the user preference $\Pr_{i-j}$ influences the final handoff decision Fo_{i-j} for connection i by (2).

$$Fo_{i-j} = W_{i-k} * R_{k-j} * \Pr_{i-j} \tag{2}$$

In (2), j represents the target network, and W_{i-k}, $\Pr_{i-j}$ are both in the range of 0-1. Similarly, the impact of device capabilities could be handled as above.

This multi-criteria algorithm takes advantages of both AHP and SAW to make handoff decision, whose performance will be analyzed in Section 4.

Step4 Action Executing

After the handoff decision for each connection gained from step 3, corresponding operations will be enforced on BSs/APs and the MT. With regard to BSs/APs, authorization for the MT to use their resources needs to be processed. For the MT, some connection entries in its CIL need to be modified.

The proposed solution is under observation. If the new case is well dealt with, the solution will be added to the CB. This is a self-learning procedure, a key step to achieve autonomicity in connection management. Along with more cases experienced by MT, the CB will get more plentiful. When the CB gets stable to some degree, new cases could be almost matched with cases in it and solutions can be directly retrieved rather than calculated by step 3.

4 Simulation Results and Performance Analyzing

Simulations were carried out in ns-2+802.21 [14] [15] to evaluate the performance of our mechanism. Fig. 4 illustrates the simulation scenario. Here it is supposed that the UMTS has full coverage while WLAN exists with access point located in (100,100), which has 50 meters coverage radius. The MT moves from (40, 100) to (160, 100) from 10s in the time axis with a certain constant velocity ($v_{\min} = 1m/s$,

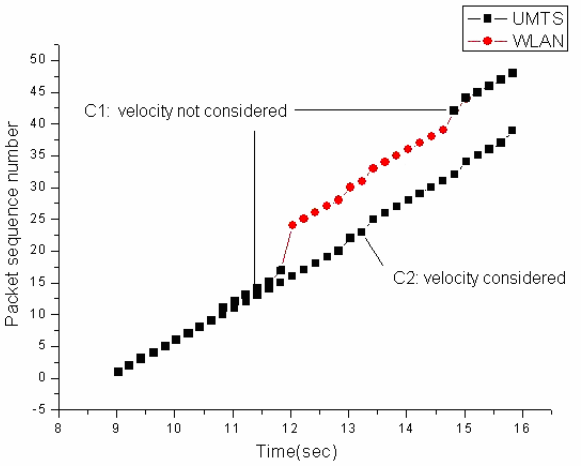


Fig. 4. Impact on packet loss rate of velocity

$v_{\max} = 30m/s$ and $v_{threshold} = 15m/s$). A correspondent terminal (CT) initiated a UDP connection with MT for data downloading, which last from 9s to 16s.

(ⅰ) Impact of MT's Velocity on Packet Loss Rate

Fig. 5 is an illustration of the packet loss rate under $v = 20m/s$, which has exceeded the threshold. As shown in Curve 1, if velocity was not considered, once WLAN was detected and a handoff decision that WLAN was more suitable for data downloading was made, a vertical handoff happened and the connection started to run in WLAN. When the MT moved out of the coverage of WLAN, the connection had another handoff and then run in UMTS again. During 9s and 16s, two handoffs happened. According to the data report in trace file, 15 packets were lost while 53 packets transmitted, so the packet loss rate was 0.28.

Relatively, velocity was taken into account for handoff decision in our mechanism. Since the velocity exceeded the threshold, whether the status of WLAN was better or not, the MT just kept on using UMTS. Curve 2 represents the packet performance when our algorithm was carried out. According to the data report in trace file, only 4 packets were lost while 44 packets were transmitted, so the packet loss rate was 0.09.

Therefore, our algorithm performs well on low packet loss rate based on velocity considered in the whole decision making procedure.

(ⅱ) Execution Time of Proposed Algorithm

If a new case can be found in the CB, the average execution time of the algorithm is less than 1ms;if not, it is between 7ms and 15ms, which includes the time spent in searching for similar cases in CB, decision making and writing a new case into CB. However, as cases in CB get more and more plentiful by self-learning, the possibility of finding a similar case in the CB is getting bigger. When the CB gets stable to some degree, the average execution time almost equals to 1ms, an idea value for multi-criteria handoff. This can obviously embodies the benefit contributed by KR.

5 Conclusions and Future Work

In this paper, an autonomic connection management mechanism is proposed, which includes making handoff decisions for connections, influencing some behaviors of the MT and BSs/APs during handoff and managing the CIL. For multi-criteria handoff decision making, an algorithm combining AHP and SAW was used. Through simulations, we can see that the mechanism reduced packet loss rate by considering an MT's velocity and CBR contributed to the short time of handoff decision.

Our future work includes the prototype validation of the proposed mechanism in heterogeneous wireless access networks.

References

1. Tanenbaum, A.S.: Computer Networks. Tsinghua University Press, Beijing (2005)
2. Mancini, E.P., Rak, M., Torella, R.: Predictive Autonomicity of Web Services in the MAWeS Framework. J. Comp. Sci. 2, 513–520 (2006)
3. Chen, L.J.: USHA: A Practical Vertical Handoff Solution. In: 3th IEEE Consumer Communications and Networking Conference, pp. 1284–1285. IEEE Press, L.V. (2006)
4. Fu, S.J., Ma, L.R., Atiquzzaman, M., Lee, Y.J.: Architecture and Performance of SIGMA: A Seamless Mobility Architecture for Data Networks. In: 40thIEEE International Conference on Communications, pp. 3249–3253. IEEE Press, Seoul (2005)
5. Badis, H., Al-Agha, K.: Fast and Efficient Vertical Handoffs in Wireless Overlay Networks. In: 15thIEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1968–1972. IEEE Press, Barcelona (2004)
6. Majlesi, A.: An Adaptive Fuzzy Logic Based Handoff Algorithm for Interworking between WLANs and Mobile Networks. In: 13th International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1223–1228. IEEE Press, Lisbon (2002)
7. Guo, Q., Zhu, J., Xu, J.H.: An Adaptive Multi-Criteria Vertical Handoff Decision Algorithm for Radio Heterogeneous Network. In: 40th IEEE International Conference on Communications, pp. 2769–2773. IEEE Press, Seoul (2005)
8. Ahmed, T.: A Context-Aware Vertical Handoff Decision Algorithm for Multimode Mobile Terminals and Its Performance. In: IEEE/ACM Euro American Conference on Telematics and Information System, pp. 19–28. IEEE Press, Santa Martha (2006)
9. Zhu, F.: Multiservice Vertical Handoff Decision Algorithms. EURASIP Journal on Wireless Communications and Networking, 1–13 (2006)
10. Chen, W.T., Liu, J.C., Huang, H.K.: An Adaptive Scheme for Vertical Handoff in Wireless Overlay Networks. In: 10th IEEE International Conference on Parallel and Distributed System, pp. 541–548. IEEE Press, Newport Beach (2004)
11. Mehbodniya, A., Chitizadeh, J.: An Intelligent Vertical Handoff Algorithm for Next Generation Wireless Networks. In: 2th IEEE/IFIP International Conference on Wireless and Optical Communications Networks, pp. 244–249. IEEE Press, Dubai (2005)
12. 3GPP: TS 23.107, V.8.0.0, Quality of Service (QoS) Concept and Architecture (2007)
13. Saaty, T.L.: How to Make A Decision: The Analytic Hierarchy Process. European Journal of Operational Research, 9–26 (1990)
14. Fall, K., Varadhan, K.: The ns manual (2002), `http://www.ecse.rpi.edu/Homepages/shivkuma/teaching/fall2002/ns-2/ns_doc.pdf`
15. Mahalingam, M.J.: Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services. In: IEEE P802.21, N.Y. (2006)

Context-Aware Connectivity and Mobility in Wireless Mesh Networks

Ricardo Matos and Susana Sargento

Universidade de Aveiro, Instituto de Telecomunicações, Portugal
{ricardo.matos,susana}@ua.pt

Abstract. Wireless Mesh Networks (WMNs) have shown a high-potential to fulfill the requirements of the Next Generation Networks (NGNs). Although mobility management is crucial to develop large-scale WMNs, the heterogeneity of today's Internet will imply a context-aware architecture in the future to optimize the users' experience. Network virtualization, as a mean to share and isolate resources, can be used as an element to construct different types of virtual networks (overlays), each one optimized for a specific set of contexts: security, mobility, Quality of Service (QoS), cost, preferences. In this paper, we present a context-aware multi-overlay architecture that enables a user to connect to the WMN that best fits its requirements and approaches. We concentrate on how to build such an architecture: how a user can move maintaining its requirements through the re-configuration of overlays, and how context can be mapped, organized and distributed in the network nodes. We also discuss the entities and the complexity of this architecture

Keywords: Network Virtualization, Wireless Mesh Networks, Multi-overlay architecture, Context-awareness, Mobility, Multi-homing, Intelligent decisions.

1 Introduction

Wireless Mesh Networks (WMNs) have emerged as a key technology for Next Generation Networks (NGNs). Traditional wired infrastructure for wireless access networks is not feasible or too expensive for many application scenarios in the near future. Replacing wired infrastructure with wireless links promotes an ease up time-to-deployment, allowing ubiquitous broadband access in a cost-effective manner.

Another emergent topic of the future Internet is the network virtualization, which brings a number of advantages, such as physical/logic separation and independence, hardware multiplexing, resource isolation and security, reliability and redundancy, and flexibility on the topology and protocols supported.

Currently, users and networks have very heterogeneous context requirements. Moreover, context information can optimize mobility performance by avoiding unnecessary handovers and long latencies, while aware of users' activity, preferences, and other context information. Integration with WMNs may offer a flexible physical infrastructure where different multi-hop paths may support several types of context.

In [1] it is presented a new approach to enable highly adaptive WMNs through the support of multiple overlays for context-based WMNs. In this approach, we model

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 49–56, 2010.

context and virtualize the WMNs by introducing multiple overlays to represent the context characteristics. Hereby, we also consider multi-homing supported by different providers and different WMNs. In this approach, a user will connect to the WMN that best fits its requirements. In this paper we show how to build such an architecture: how a user can move maintaining its requirements through the re-configuration of overlays and how this architecture can be used to optimize mobility; how context can be mapped, organized and distributed, and how the nodes of specific overlays can be discovered in an efficient way. This paper is organized as follows. Section 2 addresses the current state of virtualization and context-aware solutions over WMNs. Section 3 depicts the proposed architecture for context-based WMNs through virtualization, attempting at the management of overlays, mobility optimization and integration of context, whereas, section 4 presents the possible entities for this whole architecture as well as its envisioned complexity in real environments. Finally, section 5 concludes the paper and presents topics for further work.

2 Related Work on Context-Awareness and Overlays in WMNs

The literature contains some proposals to introduce context in WMNs. However, they are mainly focused on QoS-aware routing mechanisms [2]. In contrast, our general approach for heterogeneous networks has the potential to improve routing protocols by modeling and using different types of context, dividing a WMN into multi-overlays networks in order to provide networks that best match the different users' requirements and to optimize multi-homing. Based on the expected performance, the overlay can be setup and mapped to the physical network [3], [4]. Recent works used machine learning techniques for this purpose in WMNs [5], [6].

There are a huge number of approaches for mobility management in WMNs, aiming to support a seamless handover for the user (see as e.g. [7], [8]). Since mobility is a key requirement in any type of proposal, optimization of mobility through this multi-overlay architecture is also an objective. For a user, when it moves, it changes its physical connection; however, due to virtualization and overlay's reconfiguration, it may remain logically connected to the same logical node.

Similar to operating system virtualization, network virtualization has the potential to support multiple (logical) networks simultaneously [9]. Logical overlay networks proposing "network slicing" are, as e.g., addressed in [10] that accommodate several experiments simultaneously in space, time and frequency division manner. In [11], the authors describe an approach of a joint optimization streaming rate allocation of flows and power consumption of links for forwarding data flows in multicast overlays over WMNs. In [12], a Wireless Ring over a regular WMN is proposed in order to carry high-bandwidth data. In [13], it is proposed MeshChord, which uses location-dependent addressing schemes in order to reduce traffic for maintaining a Chord overlay over WMNs. Although these approaches use multi-overlays, they do not consider context and the corresponding open research issues: (i) how to identify and rate context characteristics and automatically map them to a network structure; (ii) how to create an appropriate number of multi-overlays; (iii) how to select the best fitting overlay; and (iv) how to adapt and maintain the multi-overlays.

3 Multi-Overlay Environment

This section presents the context-aware multi-overlay approach envisioned for highly dynamic WMNs supporting optimized users' experience in mobile and multi-homing environments. Since wireless mesh routers are meant to build well-structured networking organizations which need to fulfill several connecting targets, we introduce context-awareness along parallel virtual networks (or overlay networks). These overlays can be used to optimize the network along one or more context parameters, and to connect users that share the same or similar context. We consider different types of context: user, network, price and predicted context.

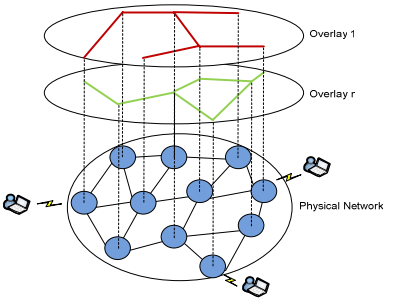


Fig. 1. Multi-Overlay Architecture for Context-based WMNs

In this approach we also consider multi-homing, supported by different providers and different WMNs, with the possibility of different users to be associated with different overlays. A first sketch of our multi-overlay architecture is shown in Fig. 1. This multi-overlay environment requires an effective solution for its management and control. We need mechanisms to select the overlays, as well as information/signaling to create/reconfigure them and to distribute the nodes through them. The creation and reconfiguration may be activated through users' mobility.

The integration of context with respect to the different entities (e.g., user, device, application, network, Internet Service Provider - ISP) in WMNs introduces several open issues and challenges that need to be addressed: overlay's characterization according to its context, and distribution of the context in the network; virtualization in wireless environments in order to decrease interference; intelligent algorithms to choose the best overlay for a user, according to the context of all entities involved, as well as, to decide between overlays' creation or reconfiguration to optimize users' experience; mapping of the overlays in the physical network, and, resources' scheduling and polling; allocation of different overlays for different user's applications, interfaces or connections (multi-homing); scalability of the solution.

The next sub-sections present the mechanisms to support the management of overlays, mobility and context-embedding.

3.1 Management of Overlays

The overlay's management has three different and important phases: (i) selection, (ii) creation and (iii) reconfiguration:

(i) *Selection of Overlays*. When a user arrives at the network consisting of a multitude of overlays, the best one should be selected for user's connectivity. In section 3.3 we present two different distributed solutions for the mapping and integration of context in the network elements, and mechanisms to efficiently find the closest node belonging to a specific overlay.
(ii) *Creation of Overlays*. If a user requires an overlay which is not already available in the network (all overlays currently available exhibit characteristics not fitting to the user's requirement ranges), the best matching overlay may be chosen or a new overlay needs to be created.
(iii) *Reconfiguration of Overlays*. Based on context, preferences, and resulting mobility management, overlays may need to be reconfigured proactively.

3.2 Mobility Optimization through Overlays

In the proposed approach, the movement of a user may require the reconfiguration of the network, through creation and reconfiguration of overlays, to enable the user to be connected to the same overlay while moving. However, the concept of overlays can also improve mobility management, since the reconfiguration of the overlay may provide the user with the same logical router. For the user, when it moves, it remains logically connected to the same mesh router (belonging to the same overlay). Therefore, with this approach, mobility just requires a change of physical connection to a different physical node (link-layer handover), being IP-independent.

Fig. 2 depicts the main processes required to optimize mobility of a user (between an old and a new mesh router) through this context-aware multi-overlay architecture. Mobility of users can be modeled or predicted and this aspect will be introduced as a context parameter. Besides network-centric mobility management, user triggering is also possible and will require similar processes. The old router needs then to attempt at the user's context, find the predicted new mesh router for the user, and send the user's context to the mesh router. The next step is the reconfiguration of overlays:

(i) First, it is verified if the old and new routers both belong to the user's overlay. If it is true, there is no need to reconfigure the current overlay and the algorithm is stopped. After paths/routing updates, the user switches to the new router.
(ii) If the new router does not contain the user's overlay, but it can be extended to the new router, the overlay is reconfigured. After overlay and paths/routing updates, the user switches its physical link to the new router.
(iii) If the new router does not contain the user's overlay, and it cannot be extended to the new router, an available and suitable overlay for the user needs to be found, in the new router or even in its physical or virtual neighbors. In this case, one virtual link is added and, after overlay and paths/routing updates, the user switches to the suitable overlay.
(iv) If the new router does not contain the user's overlay, and there is no suitable overlay in its neighborhood, a distributed decision needs to be in place.

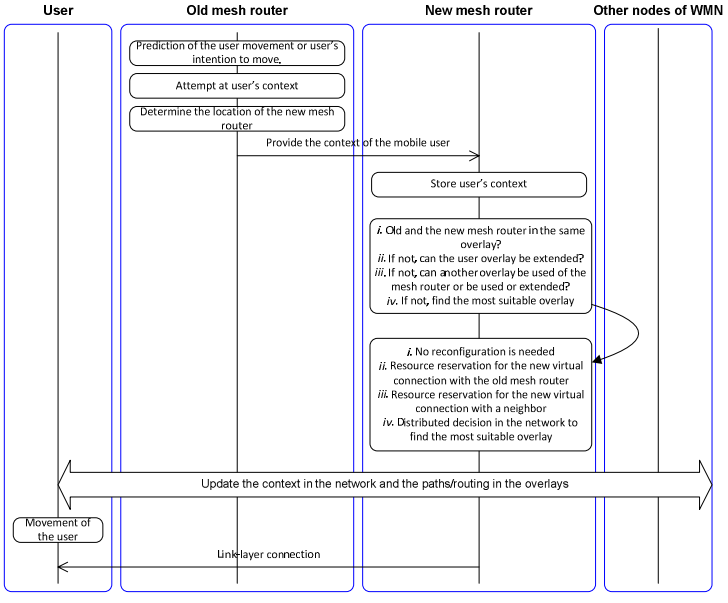


Fig. 2. Mobility Optimization through Multi-Overlay Environment

A user movement requires the update of the context in the network and of the paths/routing in the overlays. This update can be performed using the advantages of DHTs, finding an intermediate solution between the standard routing protocols for WMNs and the information that DHTs provides. As an example, the network can be divided in clusters (domains) with a DHT-based Peer-to-Peer (P2P) control overlay, where each cluster is represented by a key. These clusters have to be organized in the overlay based on their physically proximity (using "shortcuts" between them) in order to decrease the number of physical hops per overlay hop. The routing inside each cluster can be a standard WMN routing protocol.

We expect that this reconfiguration process is finished before the user's movement; when the new mesh router detects the user in its neighborhood, it is promoted an instantaneous link-layer connection.

3.3 Integrating Context through Distributed Hash Tables

The most traditional approach to store context data and resolve search requests is to use a centralized search engine. Although this approach can provide fast responses to a context query in a small network, it has limitations such as scalability, processing bottlenecks and single points of failure. P2P approaches, on the other hand, have been proposed to overcome these obstacles. They typically implement DHTs and use hashed keys to direct a lookup request to the specific nodes by leveraging on a structured overlay network. We then use DHTs' approach to organize our multi-overlay context-based environment. For this purpose, we require the knowledge of the current overlays in the network and their main features. We propose two independent solutions to integrate context through DHTs.

First solution. The overlays are organized based on their context features; users also contain their context parameters. The user's context will be matched against the overlays' properties in order to find the best overlay for a user.

The overlay's features of a cluster (domain) can be distributed in a P2P control overlay, where each peer is a router of the physical network which stores a key that represents the properties of the overlays it contains. Through this P2P overlay, an efficient lookup procedure may be supported in order to find the best overlay for a user, attempting not only at the matching of the user's and overlays' context, but also at the location of a point of attachment for a particular overlay. To support this approach, it is required to devise a mechanism to efficiently create a key, based on all types of context to describe each. One drawback of this approach can be the potentially slow lookup procedure for a large number of overlays.

Second solution. The DHT can be organized in a ring, based on context's features that characterize the overlays (see Fig. 3).

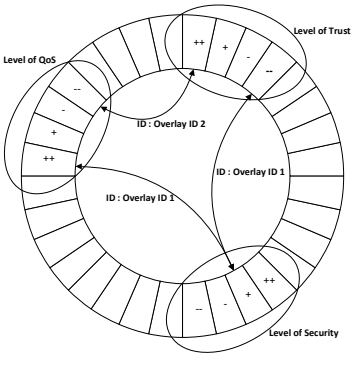


Fig. 3. Context Organization through DHTs – Second Solution

The context parameters are divided in levels/IDs (for e.g., context can be described with the following levels: QoS – 0; redundancy – 1; trust – 2; reliability – 3; etc.). Each level/ID of context can have four different sub-levels/sub-IDs (++, +, - ,--). Then, the different levels of contexts can be connected based on the ID of each data overlay, in order to represent the data overlays' features. As represented in Fig. 3, data overlay 1 is characterized by a "++" sub-level of QoS (0), a "+" sub-level of security (4) and a "--" sub-level of trust (2). In order to organize its context in our DHT, we should use "shortcuts" between these sub-levels, based on the ID of the data overlay 1.

Through this process, it is possible to efficiently and directly find several possible overlays that can be allocated to a user. However, this solution has two main drawbacks: all this information has to be presented in all nodes of a P2P control overlay of a specific domain; if the number of data overlays is large, since they can be characterized by different types of context, the number of "shortcuts" based on the ID of the same data overlay (multi-level DHTs) is also large. This may also slowdown the process of finding the best suitable overlay for a user. The bootstrapping of DHTs and the shortcuts' maintenance will need to be evaluated.

Moreover, both solutions will need to be evaluated in terms of overhead and cost. Notice that the lack of resources of wireless environments and the number of protocols at different layers in this approach may introduce challenges on the support of DHTs in this type of environments. These challenges will be evaluated and different solutions need to be investigated

Scalability of the approaches can be achieved by using two levels of P2P control-overlays: a higher level P2P overlay, where each peer represents a domain, and the lower level with the control peers of each domain (the two solutions, presented before, focus on the context-embedding inside a domain). In the higher level, each peer can be characterized by the context characteristics of the best overlay of the domain for a specific context requirement. However, there are several issues that still need to be investigated, such as the location of a peer of a domain and the size of a domain.

4 Architectural Discussion

The creation/reconfiguration of a particular overlay requires the existence of an efficient resource manager. It is also required an entity that acquires and stores the context of all entities involved. Both these entities, ***Resource Manager*** and ***Context Acquisition/Repository***, should be distributed in the network through DHTs in a P2P control overlay. The context information should reside in an abstraction layer (overlay) between the physical and the virtual environment, organized by one of the solutions presented in section 3.3. A framework for managing the user's mobility – ***Mobility Manager*** – should reside in all mesh routers, in order to predict the movement of its attached users, and trigger the reconfiguration process of the overlays. Finally, it is also required a framework that integrates the context of all entities and network resources, and promotes an intelligent overlay's management – ***Overlays Manager***. Here, the cost of each decision – create or reconfigure an overlay – should be evaluated: the matching of overlays' features and users' requirements should be performed to select, create or reconfigure an overlay; the overlay manager has to select the correct overlay's instance in each router, and coordinate all entities.

Breaking a WMN into a number of virtual overlays can introduce different types of costs. We will have management costs to create and manage the virtual networks, as well as, usual costs of loss of aggregation in virtual environments. However, the flexibility envisioned in these high-dynamic WMNs provides the optimization of user experience, enabling its connection through already established overlays with the required characteristics. The use of DHTs and network virtualization in wireless environments can introduce overhead, performance delays and signaling cost; these aspects require a carefully evaluation, and need to be compared with central approaches and other distributed mechanisms. The real number of overlays supported by a WMN, as well as, the QoS/QoE offered to a user, need also to be evaluated.

5 Conclusion

In this paper we proposed a novel architecture consisting of multiple overlays in order to integrate context in WMNs to optimize the user experience and promote

multi-homing, attempting at the advantages of network virtualization. We introduced the key challenges that need to be addressed in order to integrate context in a multi-overlay context based virtual environment, as well as solutions to optimize user's mobility, and to organize the context and the virtual networks in this architecture.

In the future, we plan to evaluate the presented solutions and to compare them against other approaches, regarding overhead and signaling costs. Moreover, we plan to measure the real benefits of this architecture and its implementation cost. Finally, the mobility of the virtual mesh routers, multi-homing and multi-path support, efficient resource management and multi-domain environments are other topics that need further research.

References

1. Hummel, K., Hess, A., Sargento, S., Matos, R., Tutschku, K., Meer, H.: Context-based Wireless Mesh Networks: A Case for Network Virtualization. In: 2nd Euro-NF Workshop on Future Internet Architectures: New Trends in Service Architectures, Santander, Spain (June 2009)
2. Subramanian, A., Buddhikot, M., Miller, S.: Interference aware routing in multi-radio wireless mesh networks. In: Proceedings of WiMesh 2006, pp. 55–63 (2006)
3. Yuy, M., Yiz, Y., Rexfordy, J., Chiang, M.: Rethinking virtual network embedding: Substrate support for path splitting and migration. ACM SIGCOOM 38(2) (2008)
4. Zhu, Y., Ammar, M.: Algorithms for assigning substrate network resources to virtual network components. In: Proceedings of INFOCOM 2006 (2006)
5. Hu, P., Robinson, R., Portmann, M., Indulska, J.: Context-aware routing in wireless mesh networks. In: Proceedings of CEASEMANS 2008, pp. 16–23 (2008)
6. Lin, T., Wang, C., Lin, P.C.: A neural-network-based context-aware handoff algorithm for multimedia computing. ACM Transactions on Multimedia Computing, Communications and Applications 4(3), 17–23 (2008)
7. Ren, M., Liu, C., Zhao, H., Zhao, T., Yan, W.: Memo: An applied wireless mesh network with client support and mobility management. In: Proceedings of GLOBECOM 2007, pp. 5075–5079 (2007)
8. Amir, Y., Danilov, C., Hilsdale, M., Musaloiu-Elefteri, R., Rivera, N.: Fast handoff for seamless wireless mesh networks. In: MobiSys 2006, pp. 83–95. ACM, New York (2006)
9. Peterson, L., Shenker, S., Turner, J.: Overcoming the internet impasse through virtualization. In: ACM Workshop on HotNets 2004 (2004)
10. Shrestha, S.L., Lee, J., Chong, S.: Virtualization and slicing of wireless mesh network. In: International Conference on Future Internet Technologies (2008)
11. Zhu, C., Wu, D., Cheng, W., Yang, Z.: Efficient overlay multicast strategy for wireless mesh networks. In: VTC 2008-Fall (2008)
12. Reaz, A., Ramamurthi, V., Ghosal, D., Benko, J., Wei, L., Dixit, S., Mukherjee, B.: Enhancing multi-hop wireless mesh networks with a ring overlay. In: SECON Worshops 2008 (2008)
13. Burresi, S., Canali, C., Renda, M.E., Santi, P.: MeshChord: A location-aware, cross-layer specialization of chord for wireless mesh networks. In: PerCom 2008, pp. 206–212 (2008)

Dissemination of Anonymised Context Information by Extending the DCXP Framework

Stefan Forsström, Victor Kardeby, Jamie Walters, Roger Norling, and Theo Kanter

Department of Information Technology and Media
Mid Sweden University
SE-851 70 Sundsvall, Sweden
{stefan.forsstrom,victor.kardeby,jamie.walters,
roger.norling,theo.kanter}@miun.se

Abstract. The increasing ubiquity of context aware services and systems has been primarily underpinned by the use of centralised servers employing protocols that do no scale well for real time distribution and acquisition of neither sensor data nor dependent services. Any shift from this generic sensor framework mandated a new thinking where sensor data was capable of being propagated in real time using protocols and data models which serve to reduce unnecessary communication overhead. DCXP is proposed as an alternative architecture for the real time distribution of context information to ubiquitous mobile services. As a P2P based distributed protocol, it inherently poses the challenge of user anonymity across the system. In this paper we briefly present DCXP along with further work to enable the anonymised dissemination of sensor information within the architecture. Such a solution would have a negligible impact on the overall scalability and performance of DCXP.

1 Introduction

Previous systems exist that provide ubiquitous access to context information both centralised [1,2] and distributed[3,4,5]. Common among these systems is that they lack the options of providing anonymisation services to their users.

Anonymisation is the act of removing all information about the sender from a transmitted message such that the recipient or the system cannot ascertain the identity of the sender. Anonymisation has been long sought after in many different situations even before the existence of computers, such as anonymous charity, anonymous tips to law enforcement agencies or the press [6].

The need for anonymity has progressed onto the Internet with various attempts at addressing it. One of the earliest anonymisation methods is the Chaum Mix [7] named after its creator David Chaum. In P2P systems several Chaum mixes, or derivatives provide one or all of the anonymity services discussed in [8]: receiver anonymity, sender anonymity and receiver-sender unlinkability.

Several concurrent research into anonymous P2P exists; some utilise a central authority to distribute public/private key pairs [9,10] others provide optional

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 57–66, 2010.

encryption [11] or no encryption at all [12]. There exists some anonymity P2P systems that uses probabilistic random walks through the structured network [12] whereas other systems uses pre-calculated routes [10]. However none of these systems are niched toward real-time dissemination of context information within sensor networks. This paper presents an extension to the novel Distributed Context eXchange Protocol (DCXP) presented in [13], to enable anonymous dissemination of context information. The goal is to provide receiver anonymity, sender anonymity and receiver-sender unlinkability through the anonymisation grade "Probable Innocence" as described in [6].

A common problem with previous solutions towards achieving anonymity on P2P networks is the reliance on an increased network signalling overhead. This was necessary since solutions were being developed to address the issue in the much broader context. By gearing towards context dissemination; we are able to simplify the protocol. We employ a token ring based structure for intra-group communication which significantly reduces network traffic between groups permitting us to realise a more novel solution that maintains anonymity while ensuring real time exchange of context information.

As with the DCXP framework, this solution is targeted at a distributed platform for the dissemination and sharing of context information. Sensors are attached to more powerful computers as well as mobile phones which participate, either directly as an active node or indirectly through a proxy node, in a distributed P2P overlay.

Section 2 will present a brief overview of DCXP. Section 3 presents our proposal to extend DCXP to add anonymity to the dissemination of sensor information. Section 4 draws some conclusions and present future work.

2 Distributed Context eXchange Protocol

DCXP is an XML-based application level P2P protocol which offers reliable communication among nodes that have joined the P2P network. Any end-device on the Internet that is DCXP capable may register with the P2P network and share context information. The DCXP naming scheme uses Universal Context Identifiers (UCIs) to refer to Context Information (CI) such as sensors that are stored in the DCXP network.

2.1 Context Storage

A network that uses DCXP forms a Context Storage (CS) that utilises a Distributed Hash Table (DHT) to map between UCIs and source addresses. The current DHT design choice is Chord, presented in [14]. The logical positions of participating nodes are calculated by hashing their IP numbers and using this value as a key. In this way each node is responsible for the hashed keys which fall between itself and their numerically nearest predecessor in the key space, again in a circular fashion.

The advantage of using a DHT is that entries can be found in $\log(N)$ time. In addition, the CS also acts as a context exchange mechanism. Clients query

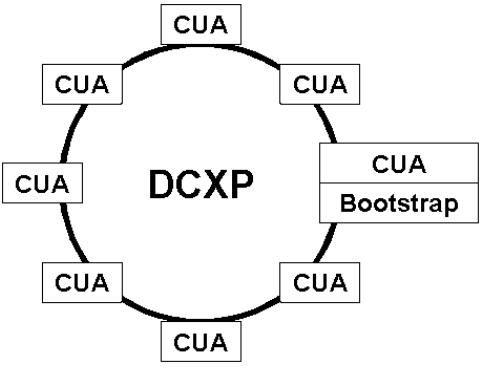


Fig. 1. DCXP architecture

the CS for an UCI to learn where the Context Information (CI) is located and the CS returns the address of the desired CI. The CS is able to resolve locations because it handles the resource registrations coming from the context sources. Thus, the CS maintains a repository of UCI/source-address pairs and provides a resolving service to the clients via DCXP. With the exception of storing CI, the operation of the CS is similar to the way that Dynamic DNS stores a mapping between a domain name and an IP address.

2.2 DCXP Topology

DCXP enables the exchange of context between sources and sinks. These sources and sinks, combined in a single end-point, is a Context User Agent (CUA). CUAs are allowed to join a context network by registering with a CS. A CUA corresponds to a node in the DHT ring that holds the CS. In particular, a CUA has a Application Programming Interface for applications and services to either resolve a UCI, get a UCI or register a UCI in the CS.

The ring in Fig. 1 symbolises the DCXP ring. Each box on the ring symbolises a node in the DCXP network, and each node has a CUA service. There can be any number of nodes in a single ring, or even a single node forming a ring with itself. The bootstrap node is the first node to be started on the DCXP network. It has to initialise and sustain the network, and each DCXP ring requires one bootstrap node.

2.3 DCXP Messages

DCXP is a SIMPLE-inspired protocol with five primitives, outlined in table 1. For more information on SIMPLE, see [15]. Fig. 2 provides an example of signaling for fetching a context value in the DCXP protocol. Each circle on the ring in the figure illustrates one Context User Agent (CUA) on the Context Storage (CS).

Table 1. The primitive messages of DCXP

REGISTER_UCI	A CUA uses REGISTER to register the UCI of a CI with the CS.
RESOLVE_UCI	In order to find where a CI is located, a CUA must send a RESOLVE to the CS.
GET	Once the CUA receives the resolved location from the CS, it GETs the CI from the resolved location.
SUBSCRIBE	SUBSCRIBE enables the CUA to start a subscription to a specified CI, only receiving new information when the CI is updated.
NOTIFY	The source CUA provides notification about the latest information to subscribing CUAs every time an update occurs or if asked for an immediate update with GET.

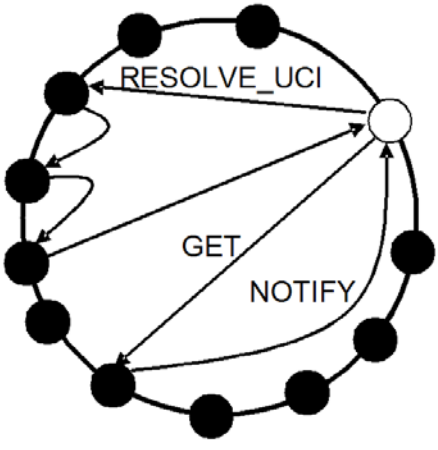


Fig. 2. DCXP signaling

2.4 Universal Context IDs

DCXP identifies each Context Information (CI) by a Universal Context Identifier (UCI) akin to a Uniform Resource Identifier (URI), as described in [16]. UCIs have the following syntax and interpretation:

```
dcxp://user@domain[/path]
```

where `dcxp` is the new URI scheme name and `domain` is a Fully Qualified Domain Name (FQDN) of the context domain. `user` provide means for ownership identification. `path` constitute a context namespace hierarchy, thus allowing for the organization and sorting of the items. An example of a fully qualified UCI would be:

```
dcxp://alice@miun.se/weather/temp
```

3 Enabling Anonymity in DCXP

In order to enable anonymous context exchange within DCXP; we propose a solution that employs a hybrid of two different anonymity approaches. Firstly, randomly selected users within the DCXP ring are grouped together communicating internally using a token ring based structure. Groups then communicate among each other in manner similar to Cashmere [9]. Since all information is sent and received as a group, individuals remain hidden inside the group. In doing so, a node achieves anonymity by the assumption of "probable innocence".

The anonymity represents an extension to the current DCXP framework as summarised in 1. The extension builds on the existing DCXP architecture, subsequently inheriting the core functionalities of system start up, initialisation and operation with the exception of the modifications detailed within this chapter.

3.1 Grouping

The grouping of users addresses some key challenges with obtaining anonymity. Users are hidden in groups making it impossible for an external user communicating with the group to identify the terminal recipient of any transmitted data. The sender's awareness is restricted to the destination's group and the random node with which it communicates. Composition of the group is achieved by subdividing the underlying DHT into smaller sub-groups. The group inherits node randomisation since the DHT's composition is determined by the hashing of node IP addresses across the network. Each group uses a token ring like protocol to construct a communication structure, such that each node is only aware of its predecessor and successor node in the token ring. By using this grouping scheme, anonymity is maintained if the group contains three or more nodes. To find the identity of an anonymous value, a malicious user must control both the predecessor or and the successor node, which is difficult to achieve since the node distribution is random by virtue of the DHT.

3.2 Changes to the UCI When Disseminating Anonymous Context

The UCIs previously mentioned in 2.3 and fully described in [17] require modification to allow for anonymity. The current UCI contains a username to identify the owner of the published context information. In order to anonymise the information, the trivial solution is to simply remove the username from the UCI. However, doing so will also remove the user context to the information thereby defeating one of the chief aims of the DCXP framework. Therefore we opt for an alternative approach of not removing the username but enabling the option of exchanging the username with an anonymous pseudonym. The pseudonym is either generated automatically to be completely anonymous or selected by the end user.

The benefits of the pseudonym is to allow a user to anonymise context information while still permitting the grouping of related context information, such as a location sensor and a co-located CO_2 sensor. The owner of the sensor remain

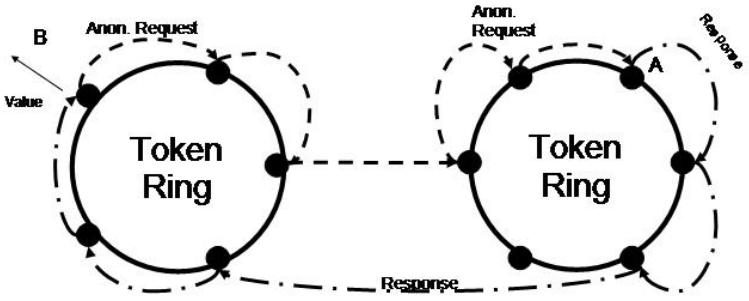


Fig. 3. DCXP Anonymous Signalling

anonymous, but the temperature sensor is given an additional context enabling a third party service monitoring CO_2 rates to benefit from the information.

3.3 Message Routing and Signaling

A token within the token ring carries both encrypted and plain text messages. On receiving a token, the node will attempt to decrypt any encrypted messages with its own private key. All successfully decrypted messages will be actioned after which all remaining encrypted messages are forwarded with the token. Plain text messages are first inspected to determine if their containing requests should be executed by this node. The remaining plain text messages are forwarded with the token as well.

However, forwarding of plain text messages may also entail delivery to the target group of the message, instead of forwarding it to the next token ring node. This choice is determined by "flipping a coin". The key benefit of this is that it increases the randomness in the structure without adding any significant overheads.

If the current node decides to deliver the message, it will further inspect and action the message depending on the message type. If however, the decision was to forward the token, then the current node simply delivers the token to its successive node which then undergoes the same decision making process.

When a node receives message from an external group, it awaits its turn for the token and delivers the message into the current token, subsequently passing the token onto the successive node. If a node encounters the same token message twice, the message is removed from the token, the assumption at this point being that the message, having made a complete round trip is either unclaimed or has been actioned.

The net outcome of this is that the source is completely unable to derive the terminal destination of the request or response data and members of the group itself are also unaware of the final recipient of the data, since nodes are simply forwarding tokens in a repeated non-discriminatory manner. Figure 3 illustrates an overview of the signalling process within the anonymity extension of DCXP.

Table 2. The primitive messages of the Token Ring

ANON_REGISTER_UCI	A CUA uses ANON_REGISTER to register the UCI of a CI with the CS anonymously.
ANON_RESOLVE_UCI	In order to anonymously find where a CI is located, a CUA sends an ANON_RESOLVE_UCI.
ANON_GET	If the resolved UCI is not anonymous the CUA uses an ANON_GET to request the CI.
ANON_SUBSCRIBE	ANON_SUBSCRIBE enables the CUA to start a subscription to an anonymous CI, only receiving new information when the CI is updated.
ANON_NOTIFY	The source CUA provides notification about the latest information to subscribing CUAs every time an update occurs or if asked for an immediate update with GET.
ANON_DIALOG_RESOLVE_UCI	In order to anonymously find where an anonymous CI is located, a CUA sends an ANON_DIALOG_RESOLVE_UCI.
ANON_DIALOG_GET	If the location of the UCI is anonymous the CUA sends an ANON_DIALOG_GET to the resolved location.
ANON_DIALOG_NOTIFY	The ANON_DIALOG_NOTIFY is used in reply to an ANON_DIALOG_GET or sent to subscribers whenever a CI value is updated if the CI is anonymous.

3.4 DCXP Anonymity Primitives

Then Anonymous Dialog messages is used for both sender and receiver anonymity while the non dialog messages only achieves receiver anonymity.

The same message names and structures as used in DCXP are adopted and extended to support the anonymous messaging protocol; see 2.3, 3.3. The primitives are detailed in table 2.

Anonymous Registration. The ANON_REGISTER_UCI, is much similar to a DXCP register except that message now contains the UCI along with its public key and it group. When a node wishes to anonymously register a UCI, it creates a register message and inserts it into the token when available. A random node in the local ring will complete the registration process with the DHT on behalf of the node.

Anonymous Resolve. An ANON_RESOLVE_UCI message is created and deposited into the token, and like the ANON_REGISTER_UCI is completed by a proxy node. The response messages are returned addressed to the group and deposited into the token to be digested by the originator.

Anonymous Get. The ANON_GET is put into the ring similar to the ANON_RESOLVE_UCI message, and is handled similarly.

Anonymous Notify. When a node executing the DCXP GET receives a reply, it constructs an ANON_NOTIFY message which is put into the token and is not removed once it has been read by the requester. The message instead traverses the ring once before it is removed. This increases anonymity in the ring and no other node is aware of the terminal recipient of the request.

Anonymous Dialogue Resolve. The resolve function when the CI provider wishes to remain anonymous differs from when only the requester desires so. The resolve is placed in the token ring as an Anonymous Resolve but the executing node retrieves the value once of the UCI it just have resolved, this value contains the group number and public key of the CI. The key and group number is posted in the token ring and allowed to circulate one lap.

Anonymous Dialogue Get. The ANON_DIALOG_GET message is much similar to an ANON_GET message with the exception that both the sender and the recipient remain anonymous. The originating node constructs the message, encrypted with the public session key of the target node along with the identification of the target group. The message is deposited in the token and passed on to the successive nodes as described in 3.3.

Anonymous Dialogue Notify. In an ANON_DIALOG_GET message, the node target node for a UCI creates a message in response to a ANON_GET. The message is encrypted using the public key of the requester and deposited in the token. The message is deposited in the token and passed on to the successive nodes as described in 3.3.

4 Conclusions and Future Work

In this paper we presented a solution for anonymously disseminating context information in a peer to peer network. We presented a solution that handles the provisioning of context data in a real-time reliable manner originating from fixed computing devices or more ubiquitous devices such as mobile phones, PDAs and laptops. We propose an extension to DCXP to provide for the distributed access of anonymous context information. This extension utilises the DCXP network to create randomised groups within which users can be anonymous under the pretence of "probably innocence". This anonymity is achievable since all users in a group act as a both proxies and terminal clients. The group uses a token ring scheme to communicate and execute data transmission operations revealing neither identities nor activity data. This results in nodes being untraceable by other nodes internal and external to the group and by extension achieving anonymity. Since there are no maximum amount of hops a message inside a token can take; a message can be carried around in the ring indefinitely. But

the coin flip algorithm will ensure that the chance of a message being delivered follows a binary distribution, therefore it is highly unlikely that a message will be indefinitely postponed.

The anonymous support presented is underpinned by a socio-technological mandate to enable the broadest participation in wide area context networks by individuals while providing the option of anonymity and privacy where required. As a distributed platform, DCXP is not afforded the centralised privacy and anonymity controls enjoyed by technologies such as the IMS infrastructure. The solution, while increasing data overhead provides a novel approach on par with centralised controls.

The token system assumes a mutual trust of all nodes inside each ring. However this exposes the ring to malicious attacks, such as denial of service. This can be achieved by always discarding the tokens or removing all messages from the tokens without forwarding them. However such denial of service attacks do not compromise anonymity within the system.

Our approach reinforces the importance of privacy regardless of the architectures employed in disseminating real-time context information and that neither has to be disadvantaged in achieving this. As we increasingly trend towards more ubiquitous computing paradigms, it gradually becomes more of a requirement to be able to involve already vast and expanding base of mobile computing users. DCXP provides an infrastructure for accomplishing this task and adding this anonymity extension allows for even greater participation of a mobile user base without requiring users to be actively involved in anonymity and privacy.

Further work to this research involves an implementation and simulation to test scalability involving issues introduced by the token ring network such as group and token sizes as well as the number of tokens in each ring.

Acknowledgment

The research is partially supported by the regional EU target 2 funds, regional public sector, and industry such as Ericsson Research and Telia.

References

1. Grosky, W.I., Kansal, A., Nath, S., Liu, J., Zhao, F.: Senseweb: An infrastructure for shared sensing. Multimedia 14, 8–13 (2007)
2. Krco, S., Cleary, D., Parker, D.: P2P mobile sensor networks. In: Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS), p. 324c (2005)
3. JXTA, https://jxta.dev.java.net/
4. Shim, E., Narayanan, S., Daley, G.: A P2P SIP architecture two layer approach, Panasonic Digital Networking Laboratory, Dallas, IETF draft (March 2006)
5. Kawakami, T., Ly, B.L.N., Takeuchi, S., Teranishi, Y.: Distributed sensor information management architecture based on semantic analysis of sensing data. In: Proceedings of the International Symposium on Applications and the Internet, pp. 353–356 (2008)

6. Kelly, D.: A taxonomy for and analysis of anonymous communications networks. PhD thesis, Air Force Institute of Technology (March 2009)
7. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24(2) (Feburary 1981)
8. Pfitzmann, A., Waidner, M.: Networks without user observability – design options. In: Pichler, F. (ed.) EUROCRYPT 1985. LNCS, vol. 219, pp. 245–253. Springer, Heidelberg (1986)
9. Zhao, B.Y., Rowstron, A., Zhuang, L., Zhou, F.: Cashmere: Resilient anonymous routing. In: The 2nd Symposium on Networked Systems Design and Implementation, NSDI (2005)
10. Goldschlag, D.M., Reed, M.G., Syverson, P.F.: Hiding routing information. In: Proceedings of the First International Workshop on Information Hiding, London, UK, pp. 137–150. Springer, Heidelberg (1996)
11. Gaurav, A.M., Oberoi, G., Post, A., Reis, C., Druschel, P.: Ap3: Cooperative, decentralized anonymous communication. In: Proc. of SIGOPS European Workshop (2004)
12. Reiter, M.K., Rubin, A.D.: Crowds: anonymity for web transactions. ACM Trans. Inf. Syst. Secur. 1(1), 66–92 (1998)
13. Kanter, T., Pettersson, S., Forsström, S., Kardeby, V., Österberg, P.: Ubiquitous mobile awareness from sensor networks. In: Proceedings of the 2^{nd} International ICST Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications (MOBILWARE), Berlin, Germany (April 2009)
14. Stoica, I., Morris, R., Karger, D., Kaashoek, F.M., Balakrishnan, H.: Chord: A scalable peer-to-peer lookup service for internet applications. In: Proc. of the Conf. on Applications, Technologies, Architectures, and Protocols for Comp. Comm., August 2001, vol. 31, pp. 149–160. ACM Press, San Diego (2001)
15. Rosenberg, J.: SIMPLE made simple: An overview of the IETF specifications for instant messaging and presence using the session initiation protocol (SIP), IETF, Internet-draft (2008)
16. Fielding, R.T., Berners-Lee, T., Masinter, L.: Uniform resource identifiers (URI): Generic syntax, IETF, RFC 2396 (August 1998)
17. Kanter, T., Österberg, P., Walters, J., Kardeby, V., Forsström, S., Pettersson, S.: The mediasense framework. In: Proceedings of th IARIA International Conference on Digital Telecommunications (ICDT), Colmar, France (July 2009)

Alternative Enhancement of Associativity Based Routing (AEABR) for Mobile Networks

Barbaros Preveze[1] and Aysel Şafak[2]

[1] Cankaya University Electronics and Communications Engineering Department, Ogretmenler cad. No:14, 06530, Balgat Ankara, Turkey
[2] Başkent University Electrical and Electronics Engineering Department, Eskişekir yolu 20. Km, Bağlıca kampüsü, Ankara, Turkey
b.preveze@cankaya.edu.tr, asafak@baskent.edu.tr

Abstract. This study proposes an alternative enhancement for the Enhanced Associativity Based Routing (EABR) method which is a derivation of ABR (Associativity Based Routing) by relative speed and relative distance estimation using the received power strength (RPS) of the nodes. In this study, it is shown that EABR outperforms some other well known protocols. The performance of EABR is improved in terms of number of route reconstructions (RRC) and connected status percentage (CSP). Message overhead and bandwidth utilization is also investigated.

Keywords: EABR, wireless, mobile, ad-hoc, routing.

1 Introduction

In an ad-hoc mobile network there are many randomly located nodes which are moving randomly from one point to another each with a random speed. Therefore, the construction of an efficient route that keeps nodes in communication for the longest time may be quite difficult. Providing maximum life for the routes causes a reduction in number of RRC (Route reconstructions). The enhancements require modifications on the tables and this will create a messaging overhead and RRC trade off. In this study, the performances of some relay selection algorithms (RSA) such as minimum distance path, minmax path, closest node to the source, path according to power threshold and path according to power threshold, EABR (Enhanced Associativity Based Routing) and the new proposed AEABR algorithm are compared in terms of number of RRC by a simulation program under the random speed, direction and initial location parameters. Messaging overhead and bandwidth utilization of these algorithms are also investigated.

2 Method

The system model has six nodes; one transmitter T_x, one receiver R_x, and four relay nodes. The area that the nodes move in is bounded with the specified boundaries and

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 67–77, 2010.

the "random waypoint model" [1] is used for the mobility of the nodes in this area. Using this model, each node in the network determines a random destination point before going to that point with a random speed. After arriving at its destination, it pauses there for a random duration and determines a new destination point to go with a random velocity. In this manner, all RSA's and long life path selection algorithms that have been worked on, make their individual selections and keep their own necessary statistics. Since all the algorithms make their decisions in the same conditions with other algorithms, it can be said that the graphs of comparison will be fair.

After simulating all the RSA's as described in section 3, their performance are evaluated in terms of number of RRC and in terms of number of making the same selection with the selection made according to path loss amount among the triangle of R_x,T_x and one of the intermediate relays.

In this study, the proposed AEABR algorithm is compared with the EABR algorithm after making a comparison of RSA's with EABR. This way, AEABR is compared indirectly with all RSA's.

3 Relay Selection Algorithms

When the node T_x tries to sent packets to R_x , a relay through which the packets can traverse will be selected. T_x always additionally uses the direct path from T_x to R_x provided that such a path is available, this way, the signals forwarded by different nodes using AAF (Amplify and Forward) or DAF (Decode and Forward) can be combined at the R_x [2]. During the implementation of the algorithms below, the distance information from each node to R_x and T_x will be needed. If GPS technology were available, the required distances could easily be taken from there as in [3] , but since it is assumed in this study that GPS is not available, the estimations of these distances are done by using the received power formula derived from Free space path loss (FSPL) given in eq. (1) [4]

$$\mathrm{FSPL} = \left(\frac{4\pi d}{\lambda}\right)^2 = \left(\frac{4\pi fd}{c}\right)^2 = \frac{P_t}{P_r} \tag{1}$$

where λ = signal wavelength (in meters), P_t = Transmitted power (in watts), P_r = Received power (in watts), c=speed of light (3x 10^8 meters / second), d=distance from T_x to Relay or R_x (in meters), f = frequency of the signal (in hertz),

By retrieving "d" from eq. (1), distance can be found as in eq (2)

$$d(T_x, R_n) = \left(c / 4\pi f \sqrt{\left(\frac{P_r(R_n)}{P_t}\right)} \right) \tag{2}$$

$d(T_x, R_n)$: Distance from T_x to R_n (meters), R_n: n^{th} relay numbered from 1 to 4, $P_r(R_n)$: Power level (in watts) received by R_n

Note that P_t has almost same value for all nodes in a small predefined range.

3.1 Minimum Distance Path

This algorithm uses eq. (2) and selects the relay through which our packets travel through the minimum distance [5]. For each possible route S from T_x to R_x

$$Path_{\min} = \min\left[(d(T_x, R_s^1) + d(R_s^{hc_s-1}, R_x) + \sum_{n=1}^{hc_s-2} d(R_s^n, R_s^{n+1})) \right] \quad (3)$$

where R_s^n : n^{th} node on the s^{th} route, hc_s : Hop count of the s^{th} route.

3.2 Minmax Distance Path

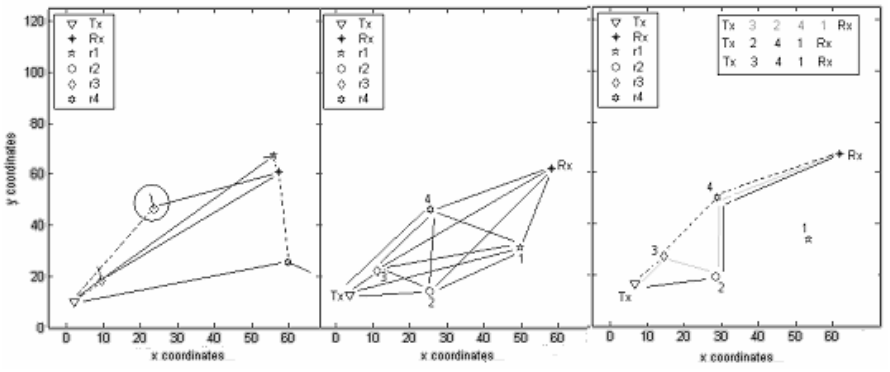
This algorithm selects the path from the set of paths for which the maximum distance between any two linked nodes of the path is lower than all other path's corresponding values, this way enough signal power level received by any node is tried to be provided [5] (See figure 1-a). The maximum partial link distance of each route numbered from 1 to S is found by eq. (4) and among these S routes, the route which returns with the lowest result from eq. (4) is selected by this algorithm.

$$Path_s = \max\left[(d(T_x, R_s^1), d(R_s^1, R_s^2), ..., d(R_s^{hc_s-1}, R_x)) \right]$$
$$Path_{\min\max} = \min\left[Path_1, Path_2, Path_3, ..., Path_s \right] \quad (4)$$

3.3 Relay Selection Using Power Threshold (PT)

In wireless mobile adhoc networks, there are algorithms such as LLRP (Longest Life Routing Protocol) that use discovery packets in order to discover to which node it has access [6] and EABR (Enhanced ABR) in which the destination sends "here I am packets" to its neighbors [7]. In this algorithm, all nodes signature a discovery packet and send it to its neighbors who will also forward these discovery packets to its own neighbors. By this way the relay from which T_x can receive R_x's discovery packet, can forward Tx's packets to R_x, and one of the relays is selected according to eq. (5) for which the Tx receives the signal from R_x with the power level greater than $Power_{Thrs}$ and other relays power levels.

$$(P_r(R_n)) = P_t \cdot \left(\frac{c}{d(T_x, R_n)(4\pi f)} \right)^2 \geq Power_{Thrs} \quad (5)$$



a) b) c)

Fig. 1. a) Minmax distance path chooses the path for which the packets will travel from source to destination via the path whose longest link is the minimum in corresponding distance values of all other possible paths, b) All possible path combinations from Tx to Rx, c) Example of selected paths as a result of EABR algorithm from Fig. 1-b).

3.4 Relay Selection According to Path Loss

If the path loss values between all node connection combinations were always known by the nodes, the nodes would directly use those paths and the path with highest average power level would be selected but it would not lead to long life routes. In order to be able to compare the results of other algorithms with the one made according to path loss, the pathloss values are calculated by eq. (6) for the connections among R_x, T_x and each relay. The relay selection is made according to this reley selection algorithm. One of the performance evaluations is the following: since the path loss algorithm selects the strongest and most reliable path, the algorithm, with selections that match the selection of path loss algorithm the most will be the best for this performance criterion, even if it has no effect on having long life route. Evaluating eq. (6) from eq.1 (1) [4]; where units are as in eq. (1)

$$\mathrm{FSPL}\,(\mathrm{dB}) = 20.\log_{10}\left(\left(\frac{4\pi\, fd}{c}\right)\right) 20.\log_{10} d + 20.\log_{10} f + 20.\log_{10}\left(\frac{4\pi}{c}\right)$$

$$\mathrm{FSPL}\,(\mathrm{dB}) = 20.\log_{10} d + 20.\log_{10} f - 147.56 \qquad (6)$$

The most important performance evaluation criterion for this study is the life time of the selected relays or paths which is inversely proportional to of number of RRC. Figure 3-d shows the number of RRC graphs of each relay selection algorithm.

4 Long Life Path Selection Algorithms

4.1 EABR (Enhanced Accociativity Based Routing)

EABR algorithm is based on associativity of the nodes as in ABR and uses the ABR algorithm [8], but in EABR, the destination has an active role in RRC, where it was passive in ABR. [9].

4.2 AEABR (Alternative Enhanced Accociativity Based Routing)

The main working principle of the proposed AEABR is a combination of ABR and EABR, and is also an implementation of ABR. The movement of the destination is also taken into the consideration as in EABR. The proposed algorithm differs from ABR in that there exist more than one path having the same number of hops in the set of possible routes determined by ABR algorithm.

In AEABR, all moving intermediate nodes in the network broadcasts “here I am” messages to all available nodes, during this period they also receive “here I am” messages which is also called associativity tick (AT), from all other nodes. These AT messages can only be received if the received power is greater than a predefined threshold power value. By seperately counting the number of AT messages received from each node and calculating an “AT threshold” value each node creates. Each node keeps its own table (see Table 1) which will be used to be informed about the state of all other nodes. The tables are updated by broadcasting discovery messages to all nodes as in LLRP (Longest life routing Protocol) [6], this way, all the nodes are aware of all other nodes tables and all available paths from Tx to Rx in the network. If one of the nodes stops sending AT messages, the corresponding field that keeps the accociativity tick of that node is reset to zero in the table, thus if the AT field is not zero, it is understood from the table that corresponding node is in the range, but having AT value greater than AT Threshold value will also be important. Since all the nodes in the network keeps the tables in the same structure, the nodes can have the indivudial neighbour availability informations of its neighbors from their tables. Once a connection is tried to be established, one of the available neighbour node is selected from the table, and during this selection an other row of the table which includes AT theshold value calculated by AT / (number of nodes) is used, this AT theshold value is continiously calculated for each node according to current state of the network and the connection through this node will be provided if AT > AT Threshold for this node.

On the other hand, the tables will also be used to discover if the node that Tx will connect to, has a path to Rx or not. The tables for a moment that Tx has no direct access to Rx, are given in Table 1.

Table 1. ABR table s of Relay 1, Relay 2, Relay 3, Relay 4, Rx and Tx

table of *R1*	R1	R2	R3	R4	Rx	Tx
Availablity	-	1	1	1	0	0
number of AT	-	3	2	4	7	0
AT Threshold	-	16/6	12/6	14/6	15/6	5/6

table of *R2*	R1	R2	R3	R4	Rx	Tx
Availablity	1	-	1	1	1	1
number of AT	**3**	-	**3**	**5**	**4**	**1**
ATThreshold	16/6	-	12/6	14/6	15/6	5/6

table of *R3*	R1	R2	R3	R4	Rx	Tx
Availablity	1	1	-	1	1	1
number of AT	2	3	-	2	4	1
ATThreshold	16/6	16/6	-	14/6	15/6	5/6

table of *R4*	R1	R2	R3	R4	Rx	Tx
Availablity	1	1	1	-	0	1
number of AT	4	5	2	-	0	3
ATThreshold	16/6	16/6	12/6	-	15/6	5/6

table of *Rx*	R1	R2	R3	R4	Rx	Tx
Availablity	0	1	1	0	-	0
number of AT	7	4	4	0	-	0
ATThreshold	16/6	16/6	12/6	14/6	-	5/6

table of *Tx*	R1	R2	R3	R4	Rx	Tx
Availablity	0	1	1	1	0	-
number of AT	1	1	3	0	0	-
ATThreshold	16/6	16/6	12/6	14/6	15/6	-

Table 2. AEABR table of Relay 4

table of *R4*	R1	R2	R3	R4	Rx	Tx
Availablity	1	1	1	-	0	1
number of AT	4	5	2	-	0	3
ATThreshold	16/6	16/6	12/6	-	15/6	5/6

+

Old Power (OP)	1,3	1,8	1,19		0	1
New Power (NP)	1,2	1,9	1,34	-	0	1

AT threshold values for nodes are calculated by adding number of AT values in corresponding table and dividing the result to total number of hops in the net, e.g. AT threshold value for R1 is calculated from the table of R1 in Table 1 as in eq (7) ;

$$R_{1_{THRS}}\left(\frac{3+2+4+7+0}{\#\ of\ nodes}\right)=16/6 \tag{7}$$

According to these tables, for a path selection from T_x to R_x, the ABR algorithm in [8] is used. According to this algorithm, the set of possible routes are determined and the one with minimum number of hops will be selected from this group. If there are more than one such route with same number of hopcount, one of them is randomly selected. AEABR comes in to consideration at this point.

We propose a method with AEABR that at first selects the routes with same number of hopcounts from these selected paths. Following this a new tabling mechanism comes into consideration, in this mechanism, two extra rows for which large buffers are not required, are added at the end of each node's own existing table as seen in Table 2. These rows includes the received AT messages power values from all the nodes in the network, the power levels of received AT messages from the nodes are periodically updated on the NP (New Power) field of the table after shifting the NP row to OP (Old Power) row, this way, the nodes will always have information about the received power changes of all nodes.

Another route selection, which will be made among the paths decided by EABR algorithm, will be done by using the OP and NP fields of their tables. Once the set of paths that came up from EABR algorithm, the tables are followed for each of these paths and average power change of all tied neighbour nodes for each path is calculated using eq. (8), for each possible route S from T_x to R_x

$$Path_{PW}=\left((Pw(T_x,R_s^{1})+Pw(R_s^{hc_s-1},R_x)+\sum_{n=1}^{hc_s-2}Pw(R_s^{n},R_s^{n+1}))/hc_s\right) \tag{8}$$

The possible path combination that can be constructed from Tx to Rx is shown in Fig. 1-b). Assuming that as a result of EABR, the 3 paths shown in Fig. 1-c) are selected. At this point, while EABR eliminates the path T_x -3 -2 -4 -1 R_x since it has more hop counts than available minimum hop counts in other paths, and randomly selecting one of the paths which has three hops, the new proposed AEABR algorithm uses NP and OP fields and makes another selection. For the state shown in Fig. 1-c), selection will be done by selection the minimum of eq. (8). Since the minimum change in received power means minimum differentiating in relative distances between these nodes, the path whose links has minimum average power differentiation

will be selected, hence the positions, directions and velocities of the notes are all taken into consideration in terms of power level differantiation, without using GPS technology.

5 Messaging Overheads of the Long Life Relay Selection Algorithms

Since 48 OFDM symbols exist in 5 ms., in total 200 frames / second will be sent. On the other hand, since there are 720 sub channels, each with 6 bits (64 QAM) [10] (720x 6) / 30 = 144 bits (without FEC) per sub channel will be sent in 5 ms. Using ¾ FEC, this ratio reduces to 108 bits per sub channel. This means a device producing 108 bits in 5 ms requires 1 sub channel.

There is an area that the nodes can make movements in, and there are some number of nodes (6 in the simulation) moving in this area, each of these nodes send the necessary information in its table to the nodes that it has access to. Thus, the number of nodes that a node access to and the messaging overhead can be calculated as the following.

For ABR, 2 integer values (2x4 bytes) and 1 floating point number (1x4 bytes) exist in the table for each of the neighbor node (Table 1) in total 12 bytes (i.e. 12x8=96 bits) information exits to send for 1 neighbor node. For AEABR, 2 integer values (2x4 bytes) and 3 floating point numbers (3x4 bytes) exists in the table for each of the neighbor node (tables 2-3) in total 20 bytes (i.e. 20x8=160 bits) information exits to send for 1 neighbor node. Since each node will send its complete table to its neighbors, the data size that will be sent is dependent on the number of neighbor nodes;

For ABR: Number of neighbors x (3x4 bytes) = Number of neighbors x 96 bits

For AEABR: Number of neighbors x (5x4 bytes) = Number of neighbors x160 bits

As seen from the calculation above if ABR has only 1 neighbor, it needs only one subcarrier and uses only 96 bits of 108 bits (without FEC) where 108-96 = 12 bits (% 11) are wasted. On the other hand, if AEABR has only 1 neighbor, it will need an extra subcarrier and uses only 160 bits of 108x2=216 bits (without FEC) where 216-160 = 56 bits are wasted, which means 28 bits (%13) in a subcarrier is wasted, but for a complete analysis for message overheads and wasted bandwidths of ABR and AEABR these values are analyzed for different number of total nodes (from 1-100) in the area and different number of neighbors of a node which can be calculated as;

$$\text{Number of Neighbor} = \frac{(\text{range of the node} \cdot \text{total number of nodes in the area})}{\text{AREA}} \quad (9)$$

where range of the node can be calculated using eq. 2 by equalizing the P_r to power threshold value.

The resultant graph for the range of message overheads and wasted bandwidths of ABR and AEABR for different number of total nodes (from 1-1000) in the area (100x120 meters) and different number of neighbors of a node is illustrated in Fig. 2.

For the case we have in our simulation ABR will send 96 bits and AEBR will send 160 bits per neighbor so the wasted bit amounts for different number of neighbors will be as seen in Table 4.

Table 3. Mobile WiMAX (802.16) data rates with PUSC sub channel (Wimax Forum) [10]

System parameter	Downlink	Uplink	Downlink	Uplink
System bandwidth	5 MHz		10 MHz	
FFT size	512		1024	
Data subcarriers	360	272	720	560
Sub-channels	**15**	**17**	**30**	**35**
Symbol period	102.9 μ seconds			
Frame duration	5 msec			

Table 4. Budget of sent bits and wasted bandwidth according to the number of neighbor count for ABR and AEABR

ABR							AEABR					
	Sent bits	96	192	288	384	480		Sent bits	160	320	480	640	800
	Wasted bits	12	24	36	48	60		Wasted bits	56	4	60	8	64
	Neigbours	1	2	3	4	5		Neigbours	1	2	3	4	5

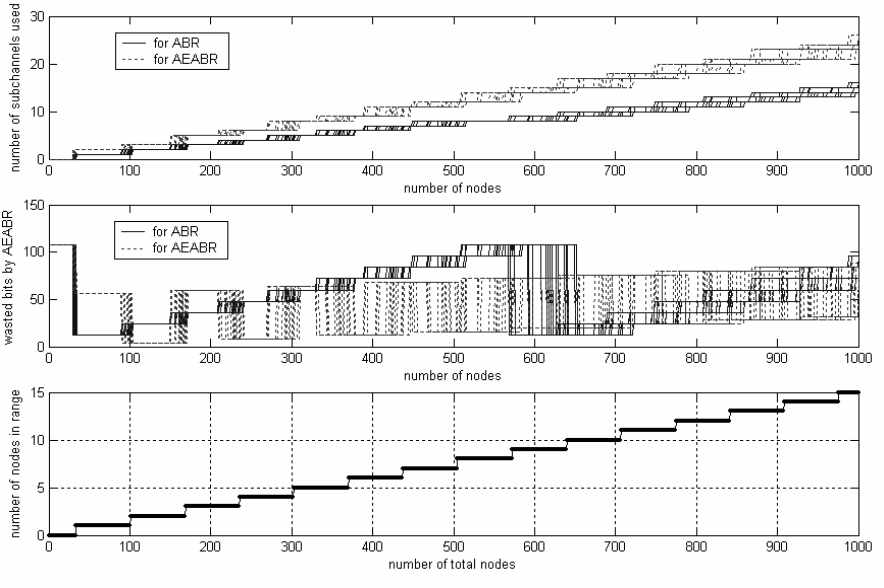


Fig. 2. The range of the message overhead, wasted bandwidth of ABR - AEABR and average neighbor count for according to for different number of total nodes and for different number of neighbors

The wasted bits values can be formulated as in eq. 10 (for ABR) and eq. 11 (for AEABR)

For ABR: $(Neighbor\ count \bmod 2)\, x12$ (10)

For AEABR:

$$\left\{ \begin{array}{l} \left\{ 4x\left[\mathrm{int}\left(\frac{Neighbor\ count}{2} \right) + 1 \right] + 52 \right\} x\left((Neighbor\ count) \bmod 2 \right) \\ + \left(\frac{Neighbor\ count}{2} \right) x4x(1 - (Neighbor\ count \bmod 2)) \end{array} \right\} \bmod 108 \quad (11)$$

6 Results and Discussion

6.1 Results of the Relay Selection Algorithms

For RSA's mentioned above, in order to be able to compare the results of other algorithms with the ones made according to path loss values, the path loss values are calculated using eq. (6) for the connections between R_x , T_x via each of the relays. Relay selection is made according to path loss RSA. In one of the performance evaluations, the algorithm with most selections matching the selection of path loss algorithm will be the best for this performance criterion. In Fig. 3-a), the result of the simulation

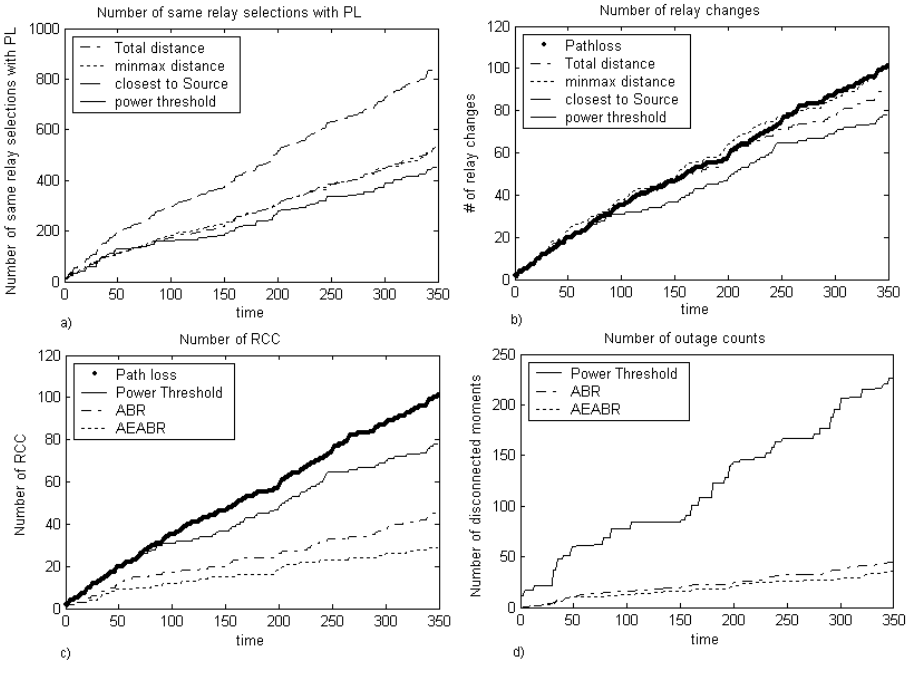


Fig. 3. a) Number of relay selections that matches the selection done according to path loss b) Number of RRC for each RSA c) Number of RRC for path loss, power threshold, EABR and AEABR d) Number of moments that T_x and R_x couldn't get connected (TRCC)

which is also reached in [2], indicate that, since its selections match the path loss algorithm's selections the most, the best selection with minimum path loss are made with the "closest to source" algorithm.

Another performance evaluation criterion for RSA's is the life time of the selected relays or paths which is inversely proportional to number of RRC. Fig. 3-b) shows the number of RRC graphs of each RSA. Since PT has minimum number of RRC's in Fig. 3-b), it is clearly seen that the PT algorithm is one of the best algorithms. From the results from Fig. 3-c) and Fig. 3-d), it can be deduced that, using PT in AEABR is a good choice, that is why the received power level is used in acceptance of received AT's and making the desicion according to average power change of all links in each path in eq. 8 and min of eq. 8.

6.2 Results of the Long Life Path Selection Algorithms EABR and AEABR

As a result, it is seen in Fig. 3-c) that the newly proposed algorithm provides a % 34.78 decrease in number of RCC's from 46 to 30 in 350 seconds from the performance of EABR which also has much better performance than path loss relay selection algorithm. Since the PT relay selection algorithm is one of the best of RSA's according to Fig. 3-b), EABR and AEABR are indirectly compared with all other RSA's in terms of number of RRC's, and it is seen in Fig. 3-c) that AEABR has the lowest number of RCC and it has the highest performance. Note that more than one intermediate node can be used in path constructions when necessary. On the other hand, in the proposed algorithm, while the numbers of RRC's are reduced, the number of moments that T_x and R_x couldn't get connected (number of TRCC) at least must not increase even if it does not decrease. From Fig. 3-d), it is seen that this condition is also satisfied by AEABR, because the line of AEABR mostly lies below the line of EABR line in time vs. TRCC graph.

7 Conclusion

An alternative enhancement for Accociativity Based Routing algorithm is developed and compared with EABR (Enhanced Associativity Based Routing). It is seen that AEABR (Alternatine Enhancement on Accociativity Based Routing) has higher performance than EABR which also has much more better performance than all other well known single hop relay selection algorithms such as minimum distance path, minmax path, closest node to the source path according to power threshold and path according to path loss. It is also seen from the results that the links on the paths constructed by AEABR can stay conneced for more time than all other algorithms including EABR (see Fig.3-d).

On the other hand, it is also seen from figures that, usage amounts of some relay 1 does not differ for EABR and AEABR, while it significantly differs for relays 2, these conditions are directly dependent on both speeds of the nodes and if the moving relays are in opposite directions or in the same direction with T_x or R_x. During all these improvements there is a tradeoff between the message overheads and reducing the number of route reconstructions. As seen from figures that, the number of sub carriers used by AEABR increases by increasing neighbor count, but even AEABR uses 2 sub

channels where ABR uses only one for a single neighbor, this rate reduces to two third for greater number of neighbors, another important point that worth to investigate is the amount of the wasted bits in the sub channels during the transmission. Tables show the sent and wasted bits in a 802.16 network for which the values can be calculated using derivations. Another important point for the amount of wasted bits in the sub channels is, AEABR wastes less bandwidth if the number of neighbors of the node is between 5 -9 or greater than 15, which corresponds to 300-600 nodes and 1000 nodes in the area respectively. Also, it is also noticeable that AEABR has a wider range of wasting bandwidth and has always lower minimum values than ABR where maximum values are almost always greater.

References

1. Deborah, E., Daniel, Z., Li, T., Yakov, R., Kannan, V.: Source: Demand Routing:Packet format and forwarding specification (version 1). Internet Draft, Work in progress (January 1995)
2. Meier, A.: Cooperative Diversity in Wireless Networks, Erasmus Project at theUniversity of Edinburgh
3. Kim, D., Toh, C.K., Choi, Y.: Location-aware long liferoute selection in wireless ad-hoc networks. Electronic Letters 36(18) (August 31, 2000)
4. Wikipedia, http://en.wikipedia.org/wiki/Free-space_path_loss
5. Sreng, V., Yanikomeroglu, H., Falconer, D.D.: Relayer Selection Strategies in Cellular Networks with Peer-to-Peer Relaying. In: 2003 IEEE 58th Vehicular Technology Conference, 2003. VTC 2003, October 2003, vol. 3, pp. 1949–1953 (Fall 2003)
6. Chul, S., Woo, M., Singh, S.: Longest Life Routing Protool (LLRP) for Ad Hoc Networks with Highly Mobile Nodes, IEEE Xplore
7. Shaar, S., Fawaz, A., Murad, A.M., Ayman, M., Al-Shalabi, R., Kanaan, G.: Analysis of Enhanced Associativity Based Routing Protocol. Journal of Computer Science 2(I2), 853–858 (2006)
8. Toh, C.K.: Associativity-Based Routing for Ad-Hoc Mobile Networks. Kluwer Academic Publishers, Dordrecht; University of Cambridge, Computer Laboratory, Cambridge CB2 3QG, United Kingdom Wireless Personal Communications, vol. 4, pp. 103–139 (1997)
9. Murad, A.M., Al-Mahadeen, B.: Simulation of the Enhanced Associativity Based Routing Protocol for mobile Ad-Hoc Networks (MANET). Journal of Computer Science 3(6), 441–448 (2007)
10. Kumar, A.: Mobile Broadcasting with WIMAX. Elsevier Inc., Amsterdam (2008)

Session 3:
Future Internet

Towards Automized Interconnection of Networks: Composition and Dynamic Negotiation of SLAs

Martin Johnsson[1], Maria Ángeles Callejo Rodrígues[2], Thi Mai Trang Nguyen[3], Petteri Pöyhönen[4], and Zohra Boudjemil[5]

[1] Ericsson AB, Isafjordsgatan 14E, 164 80 Stockholm, Sweden
martin.johnsson@ericsson.com
[2] Telefónica I+D, Emilio Vargas nº 6, 28043 Madrid, Spain
macr@tid.es
[3] University of Paris 6, LIP6 – 104 Avenue du Président Kennedy, 75016 Paris, France
Thi-Mai-Trang.Nguyen@lip6.fr
[4] Nokia Siemens Networks, Linnoitustie 6, 02600 Espoo, Finland
petteri.poyhonen@nsn.com
[5] Waterford Institute of Technology, Waterford, Ireland
zboudjemil@tssg.org

Abstract. The world of telecommunications shows clear trends towards increasing dynamicity; new types of networks, new types of applications, and also new types of businesses and business relations. At the same time, and partly due to the increase in dynamicity, operators and service providers, as well as other new type of players such as access aggregators seek to find new innovative architectures, methods and technologies to decrease the cost of operating and managing networks and services. This increase in OPEX is due not only to the increasing dynamicity but also due the ever increasing number of applications. This paper provides background and overview of the underlying issues, which then is used in order to describe concepts and technologies that could play a fundamental role in addressing and resolving those issues, both from recent as well as ongoing research. The paper ends with some conclusions, and with an outlook of issues that needs further studies in upcoming research activities.

Keywords: Architecture, management, composition, SLA, negotiation, stratum, ambient networks, governance, automization.

1 Background

In the area of telecommunications such as cellular systems, as well as within data communications like the Internet, different networks interconnect in a way that requires substantial manual work. Not only does it require the setup of network nodes to configure a huge amount of different parameters concerning for example routing, traffic management, and policies, but also the negotiations of a business agreement and the SLA (Service Level Agreement) that governs the interconnection of the networks. As this consumes lot resources, it becomes increasingly difficult to handle and

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 81–92, 2010.

scale the operations and management of networks when the business and technology environment becomes more and more complex and dynamic.
During the last couple of years we have seen a tremendous growth in applications and services, and we also see trends in that we get more options regarding what access network technologies that can potentially be used at different locations, for example Turbo-3G, WLAN, and WiMAX. This has also resulted in new types of business players such as access network providers or roaming brokers.

Looking ahead there are no signs that the increased dynamic nature of networking and business will slow down. What this means is that the current procedures for internetworking needs to be more cost-efficient and scalable, as well as the ability to cut lead times for deployment of new functionality. Generally this speaks in favour of automizing many of the procedures that today require manual work.

Though the focus in the descriptions above has been on the network operator side, the possibility of automizing the interconnection of networks is uttermost a matter of improving the end user experience, and ensures that consumers have access to up-to-date and the latest developed applications and services.

This paper describes approaches to address the needs of automization of the procedures to interconnect networks that have been undertaken mainly in the research community. It also describes the most recent results and findings from work in EU-funded projects, notably 4WARD (www.4ward-project.eu), Ambient Networks (www.ambient-networks.org), and ONE (one-project.eu).

Section 2 describes important issues in internetworking which motivate to drive research beyond current state-of-the-art. Section 3 describes composition and negotiation concepts, as well as how to control and support the process of composition. Section 4 describes a use case to show how the pieces fit together, and finally Section 5 provides conclusions.

2 Issues in Current Operations and Management of Internetworking

As Ronald Coase argued in 1959 [1] that private negotiated arrangements are frequently superior to regulated arrangements in multiple fields. This has been also the case in current IP interconnection models. This has led to the existence of multiple models for the interconnection charging models as reported in [2], where different interconnection models between carriers and the negotiated services are described.

It should be noted that just for the configuration of these agreements that are performed off-line and are not done dynamically some manual configurations (or ad-hoc configurations) are still required to configure border routers in the different domains (e.g. configuration of neighbors in the BGP routers). Therefore, the procedures to negotiate a new private agreement and its configuration have a cost that could be reduced by means of the automization of all these procedures.
Moreover, considering the current trends in the evolution of the traffic ([3]), it is more or less clear that there is a huge increment of the end users' demand of new multimedia applications that require better network performance, different traffic profiles (i.e. the asymmetry of the traffic patterns is changing) or guaranteed Quality of Service (QoS), such as on-line gaming, video streaming or videoconference.

Therefore, new networks able to provide more capabilities in terms of bandwidth, network guarantees (end-to-end QoS parameters), etc. are foreseen in Future Internet scenarios. Moreover, in these scenarios, the cooperation between service providers and network providers will be also required in order to provide carrier class services across Internet. This has an important operational cost in today's networks, since as shown in [4], there are multiple solutions to provide QoS guarantees that are not only technology dependent but also vendor dependent and that, therefore, require the specification of ad-hoc solutions due to the lack of well-known interfaces and protocols.

In order to assure the success of Future Internet, all these advanced capabilities aware networks must be able to interwork in an efficient way from both the technical (the capabilities should be maintained across different domains and the agreements should be done and configured automatically) and economical point of view (operational costs must be reduced). In this context the concept of composition is interesting since as explained in the next section, it allows the automized internetworking across different domains.

3 Concepts and Technologies Supporting Automized Internetworking

3.1 Overview

The first more significant step to provide an overarching framework for the dynamic interconnection of networks was formulated and described by the Ambient Networks project. It was coined Network Composition, and in its core there is a process that describes how the Ambient Control Spaces of two Ambient Networks interconnects to form a Composition Agreement. As an extension to this work, a study was performed in 3GPP to describe Network Composition in the context of 3GPP, and how it could be useful and beneficial for the development of business and technology based on a 3GPP network architecture [5]. An interesting observation from this study acknowledges that Composition Agreements needs to be based on what is called a Framework Agreement, pointing to the fact that not "everything" can be automized, e.g. regulatory and legislative aspects needs to be settled prior to the essential business negotiation.

In the 4WARD project, a what can be called a "network algebra" has been defined which out from the Nth Stratum concept [6] describes how strata can be composed and where such composition of strata would be under the control and supervision by a Governance function. The Nth Stratum concept systemizes and generalizes the idea behind Network Composition as defined by Ambient Networks into a set of generic operations. In addition, the Nth Stratum concept also provides support for service composition, thus aiming at a unified approach to composition of network functionality.

3.2 General Composition Principles

Composition in networking can be divided into three categories: Protocol composition [7], Network composition [8], and Service composition [9, 15]. In other words,

composition in networking can be realized at three levels: protocol level, network level and service level.

Protocol composition deals with the composition of algorithms and message exchanges to build a protocol between sender and receiver. Protocol composition also deals with the combination of simple protocols to form a more complex protocol.

Network is a set of communication entities (nodes) and a set of links and associated protocols used between them. Network Composition deals with the interconnection of networks and how to compose the functionalities represented by the communication entities.

Service is defined by a set of service primitives at an interface, and is indeed independent of how that service is provided by underlying protocol or network. Service composition is thus a matter of composing the service primitives of the services to be composed.

Protocol composition can occur in design-time or in run-time, and which is also the case of Service Composition. Network Composition generally takes place during run-time. Throughout the rest of the sections below, the focus is mainly on Network Composition, but also with examples and discussions around Service Composition.

3.3 Network Composition in Ambient Networks

In the Ambient Networks project, a new framework to dynamically establish cooperation between entities called Network Composition [10, 11] was developed. Cooperation between networks requires basic interconnectivity between cooperating entities as control plane functionalities and such interconnectivity does not always exist, thus it needs to be established on the fly. The composing networks exchange their offers and requests on capabilities, resources and different kinds of services to find out whether there are sufficient incentives to compose. The Network Composition process consists of the following phases; *Media Sense, Advertisement & Discovery, Security and Internetworking Connectivity Establishment, Composition Agreement (CA) Negotiation* and *CA Realization.* These phases are not always executed in a one-way fashion, thus the process could have different forms depending on the use case for where the process is applied.

There are four composition types according to which networks can compose; 1) Network Interworking, 2) Control Delegation, 3) Control Sharing and 4) Network Integration. These types are defined based on how the composed resources are managed after a composition. In Figure 1, two Ambient Networks AN1 and AN2 have composed and a new virtual network AN12 is created. Resource *r1* is contributed according to the *Control Delegation* type, where AN1 delegates the resource control to AN2, i.e., after the composition, from management point of view, *r1* could be seen as the resource of AN2. Resources *r2* and *r3* are contributed according to *Control Sharing* and their management is the responsibility of a new resulting network AN12. Resource *r4* follows the *Network Interworking* composition type, where AN1 has granted usage rights of it, but AN2 retains its full management and control rights. The *Network Integration* type is the case where the composing networks are not visible from outside anymore after the composition, thus they can be seen as a new network.

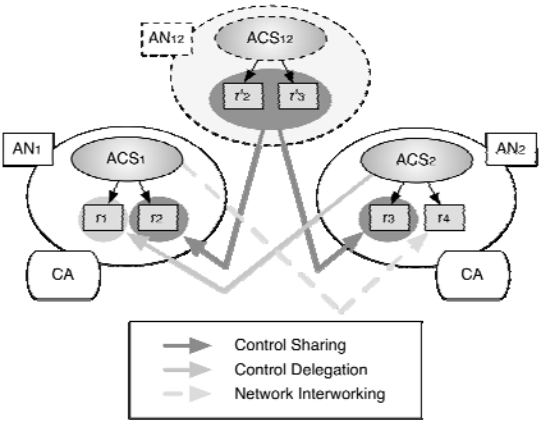


Fig. 1. Network Interworking, Control Delegation and Control Sharing composition types

Network Composition is thus about how to manage and use resources according to the agreed CA. Once the networks are composed and the CA is created, then the SLAs could be negotiated based on the CA, which basically defines how the resources could be used in the SLAs as illustrated in Figure 2. For the SLA creation, the involved entities and the used interfaces could be different compared to the CA creation. A SLA renegotiation could occur without that the related CA is changing. Thus, Network Composition between two networks can be seen as an enabler to automatically create SLAs between networks, i.e. connectivity and other networking resources based on which SLAs are negotiated are setup by Network Composition. Compared to how SLAs are used nowadays, the CA could potentially include much more technical and business details, since it is not only about services, but also more generally about resources. And this is one reason why there could be more content-wise richer SLAs that could also be temporary and created on the fly.

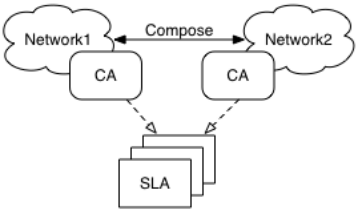


Fig. 2. The relation between CAs and SLAs

3.4 Composition Principles in the Nth Stratum Concept

The Nth Stratum concept was first described in [6], and then further developed and detailed in [12]. A stratum is defined as a distributed function which has an internal and an external view. The internal view of a stratum comprises a set of logical nodes and a medium ensuring the data transfer between the logical nodes. A logical node

models a piece of the functionality as defined for a stratum. The external view of a stratum comprises the Stratum Gatewaying Point (SGP) through which a stratum interconnects with other strata of similar type, and the Stratum Service Point (SSP) through which the services of a stratum are offered to other dissimilar strata. Figure 3 presents a stratum with its internal view and external view.

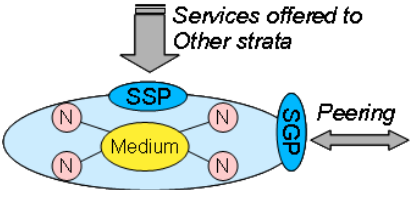


Fig. 3. Stratum with its internal and external views

The Nth-stratum framework also defines an architecture comprising vertical, horizontal strata, and abstract strata [6]. A functioning network is composed of a set of horizontal strata and vertical strata. Horizontal strata provide the connectivity and eventually additional services such as QoS, mobility or security support. Vertical strata comprise one Governance stratum and one Knowledge stratum ensuring the management and control of the horizontal strata. Abstract strata (not further described in this document) are defined in the framework as modular design patterns used to constitute horizontal and vertical strata.

Stratum is a powerful concept to model an administrative domain and how such domains can be composed. As presented in [6], horizontal strata are managed by the Governance and Knowledge strata. That means that these horizontal strata and associated Governance and Knowledge strata should be under the same administrative domain. A domain is characterized by the following properties: (i) all the components inside the domain belong to just one administrative entity, (ii) different policies can be applied inside the domain (iii) the domain provides a set of services to the end users and to other domains, (iv) the domain is autonomous in the sense that it is able to negotiate agreements with other domains. Taking into account the external reference points provided by each stratum, the SSP and the SGP, it should thus provide a clear interoperable framework.

The composition of strata belonging to different administrative domains requires a negotiation between their Governance strata (as explained in the next section). Interoperability between domains such as QoS class definition should be also resolved during the negotiation between Governance strata.

The Nth-stratum framework currently defines six generic operations: stratum instantiation, strata concatenation, strata merging, strata slicing, strata aggregation, and stratum split [12]. These strata operations can be used to control or manage the composition or decomposition of networks and services. *'Stratum instantiation'* operation instantiates a stratum over physical network, e.g. we apply IP over a set of nodes in order to form an IP network. *'Strata concatenation'* operation (maps to the Network Interworking and Control Delegation composition types) concatenates two strata, e.g. we interconnect two IP networks by border routers. *'Stratum merging'* operation (maps to the Network Integration composition type) merges two strata to form a

single stratum, e.g. the merging of two IP networks to form a single IP network. *'Strata slicing'* operation (maps to the Control Sharing composition type) is basically a virtualization operation, e.g. the allocation of an IP-based VPN. *'Strata aggregation'* operation aggregates the resources of two or more strata in order to provide a summarized representation of the resources and services available across the aggregated strata, e.g. to aggregate the routing tables in several IP networks. *'Stratum split'* operation splits a network into two networks, e.g. the division of one IP network into two separate IP networks.

Following the Nth Stratum model, the following composition types are considered:

- **Service Composition:** strata of different nature can compose via their SSPs in order to provide a specific service. This type of composition was not studied and defined in Ambient Networks.
- **Network Composition:** strata of the same nature compose in order to extend a specific service entity to another network environment. In this case, both strata negotiate and implement the agreement through the SGP.

3.5 Governance for the Control and Supervision of Composition

The Governance Stratum is in charge of managing the operation and configuration of the Horizontal Strata, according to the specific policies defined by the network administrator. The Governance stratum is supported by the Knowledge stratum that provides the functionalities related to the maintenance and monitoring of network status, including what services/resources are available in each of the horizontal strata.

Since the Governance stratum is in charge of managing the network domain, it is the main responsible for the orchestration of the composition process. In particular the following functionalities related to the composition are foreseen:

- Management of the CA including the SLA(s): the Governance stratum is responsible for the negotiation of the agreement (via the SGP of this stratum) and of the admission control process that should be triggered when a new service request is received.
- The policies as well as the network status from the Knowledge stratum, form basis for accepting or rejecting the CA. The configuration of these policies can have associated a non-dynamic operation that are required as part of the Framework Agreement where specific regulatory constraints are considered.
- Once the CA has been accepted, the Governance stratum is in charge of triggering the configuration of the Horizontal strata; this includes the authorisation of information coming from other domains that, for security reasons, must be filtered in the borders of the domain.
- The Governance stratum will also ask the Knowledge stratum to monitor the fulfilment agreement and, if an alarm is received, the Governance will take the actions required to maintain it by means of configuring the appropriate network resources.

An important step beyond the current state of the art is the interworking between domains that could implement different functionalities and services, such as for example network operators implementing the traditional transmission functionalities and service providers (providing, for example server farms to provide their services).

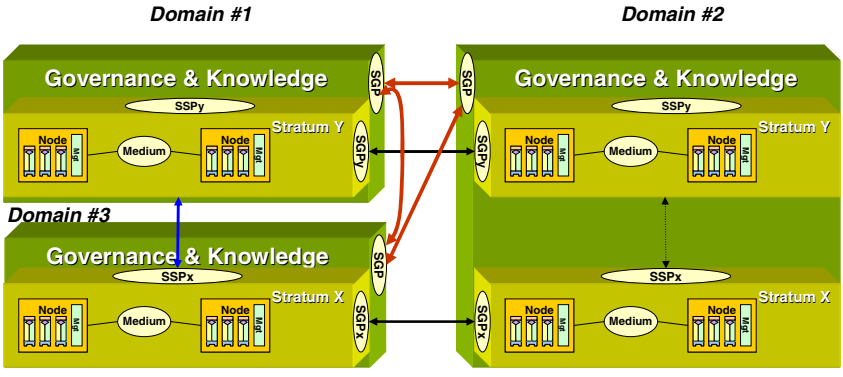


Fig. 4. Interoperability of different domains

In Figure 4 Domain #1 and Domain #3 have completely different functionalities (e.g. Domain #1 could be just an Information network with a set of nodes that are in charge of distributing the information while Domain #3 is in charge of providing transport capabilities). In this case, if Domain #2 aims to use Domain #1 services, the following interaction are foreseen:

1. Domains #1 and #3 have an agreement negotiated by means of the Governance capabilities to allow Domain #1 the usage of the services provided by Domain #3 through the SSP. The configuration of this agreement results on the composition of the services available in domains #1 and #3, which is implemented as a strata aggregation or merging, depending on the type of agreement.
2. Domains #2 and #3 have an agreement to assure the Interconnection (network composition implemented through a strata concatenation operation) for the capabilities located in the stratum X. This agreement has been negotiated through the SGP of the Governance strata (red line between domains #2 and #3) and triggers the configuration of the SGPs located at the strata X to allow the interaction between these two domains.
3. Domains #1 and #2 have an agreement to interconnect the capabilities located at strata Y. This operation follows the strata concatenation process.

In this way, Domains #1 and #2 can offer a service to, e.g. end users. This illustrates how the 4WARD Architecture Framework allows both the configuration of network and service composition allowing the implementation of multiple business agreements. The 4WARD Architecture Framework allows the Interconnection at different levels between two different domains; providing the basis for the assurance of end-to-end services. This interconnection is possible thanks to the existence of management functionalities (Governance and Knowledge) and interdomain interfaces (SSP and SGP).

This is an important achievement from both the technical and the business point of view, since in the current IP Interconnection market only two types of horizontal agreements are being considered: peering (two operators agree on processing the traffic that starts and ends in these domains) and transit or hub (a transit domain, usually a Tier-1 carrier provides connectivity to any domain). There have been other

initiatives, such as the IPX promoted by the GSM Association to design the agreements at also the service level, but this framework assumes the vertical integration of the operator, without providing enough flexibility to configure all the possible scenarios (with a lot of players) foreseen in the Future Internet.

3.6 A Meta-model for the Negotiation of Compositions

By applying the Open Negotiation Metamodel (ONM, [13]) to the CA Negotiation phase of the composition process, we allow for an automated and flexible negotiation process. This metamodel have been developed in the European IST project ONE [14]. It is designed as a tool supporting system designers in creating specific and customized negotiation models.

ONM defines all elements of a customized negotiation model and their relationships, essentially by capturing the semantics of an e-negotiation domain [14]. It covers two aspects: 1) the *negotiation information*, focusing on the *subject* of the negotiation and the negotiable *issues* depending on the business context and, 2) the *negotiation process*, defining the mechanism under which the interaction between parties takes place (the communication *process*, and *rules* governing the process).

The ONM allows designing processes for specific negotiation types but generic with respect to the actual negotiation context (such as network protocol aspects).

Figure 5 shows the core concepts of the ONM. Every *negotiation* involves *participants* (maps to Governance stratum) that negotiate towards *agreements*. The participant is represented by software where its behavior is defined by the explicit set of actions defined by the negotiation process and constrained by the negotiation rules (acceptance and rejection policies). Every *negotiation* comprises a number of *subjects* (maps to resources), which in turn contain *issues* (negotiable characteristics of such resources), which in turn are resolved by the *agreements* the *participants* are trying to reach.

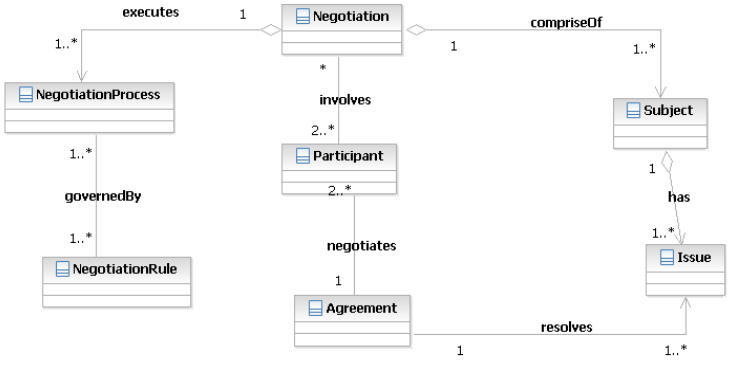


Fig. 5. Negotiation MetaModel Overview

The left part of Figure 5 shows the negotiation protocol part. Each *negotiation* executes a *process* which is governed by *rules*. The *process* will implement the behavior of the negotiation [13], and the exact messages of the negotiation protocol. The *rules* will govern this behavior according to the requirements of the negotiation information

and protocol. For this article, we assume that a policy-based management system (inherent to the Governance stratum) will provide the rules according to the context of the involved networks (and their administrative domains). ONM defines a specification language to define different CA templates and specific negotiation processes that can be used in conjunction with the Governance stratum capabilities.

4 Use Case, Putting the Pieces Together

The use case is depicted in Figure 6 below, and which we believe would be relevant to solve through network composition using the model of strata as to address issues of scalability in regard of management and also ease of use.

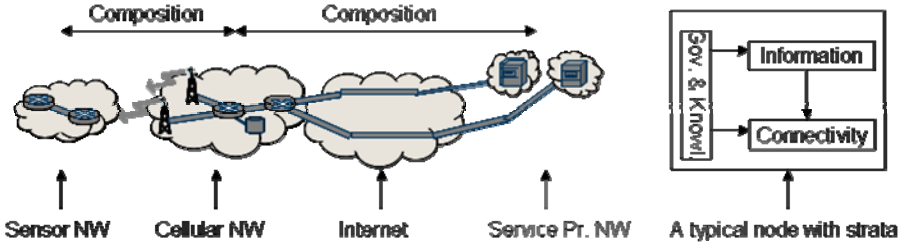


Fig. 6. The use case, with involved networks, and the strata in a node

We can here think of small sensor type of networks at the very edge, and which may well be counted in millions globally, providing some type of measurement data, e.g. weather related data. Those networks are connected via a cellular network, which could provide an aggregation and filtering service, to a service provider type of network (located somewhere on the Internet) consisting of servers which further aggregates, filters, processes, and stores the measurement data received from all the sensor networks at the edge.

The networks consist of network functionalities modeled as strata deployed across the nodes in each of the networks. Figure 6 shows a simplified view on what strata that may run in one node (real networks would consist of more horizontal strata). Governance and Knowledge strata have already been presented above. The Connectivity stratum provides connectivity services, and the Information stratum manages measurement data (this latter stratum only needs to run in nodes which manages the measurement data). The gatewaying type of nodes that needs to be present in each of the networks implements the SGP of each stratum. Notably the SGP of the Governance stratum can basically implement and execute the network composition process. Via the Knowledge stratum, the Governance stratum can find out which services/resources are available within the network and which thus can be advertised to another network (subject to policies). To establish the security association, as well as serving needs for compensation, SIM-based credentials can be used (at least between the sensor and the cellular networks). To establish the CA, ONM is applied and where specifically the services/resources related to the measurement data are negotiated. As for compensation, the owner of the sensor network may get a discount on the voice

services, and the cellular network could be compensated by getting some share of the income from ads being generated by the service provider.

Please also note that generally all the strata in the connecting networks are being composed, and thus not only the Governance strata, but their respective composition processes will be firstly under some control from the Governance stratum (and subject to policies), and secondly be a simplified version compared to the full composition process executed between the Governance strata.

In this use case, all the strata will be composed according to the strata concatenation operation.

5 Conclusions

In this paper we have described how concepts from the Ambient Networks, ONE, and 4WARD projects can be used in an integrated way to provide a solid foundation to dynamically interconnect networks. Nonetheless, though significant and mostly theoretical results have been achieved so far, there are issues left for further study, and notably further studies for how to model service composition is needed, as well as through experiments evaluate performance and scalability aspects.

Acknowledgements

The authors like to acknowledge the work of Ambient Networks, ONE, and 4WARD projects that have contributed and still (4WARD) contribute to the development of the concepts presented in this document.

References

1. Scott Marcus, J., et al.: The Future of IP Interconnection: Technical, Economic and Public Policy Aspects (January 2008)
2. Mitchel, B., et al.: Economic Study on IP Interworking, GSM Association (March 2007)
3. Cisco, Global IP Traffic Forecast and Methodology 2006-2011 (January 2008)
4. Callejo, M.A., et al.: Bridging the Standardization gap to provide QoS in Current NGN Architectures. IEEE Communications Magazine (October 2008)
5. Network Composition Feasibility Study. 3GPP Technical Report 22.980, v8.1.0 (June 2007)
6. Johnsson, M., et al.: Towards a New Architectural Framework – The Nth Stratum Concept. In: Proceedings of the 4th International Mobile Multimedia Communications Conference (MobiMedia 2008) (July 2008)
7. Men, S., Cuvellier, X., Grégoire, C., Schiper, A.: Appia vs. Cactus: Comparing Protocol Composition Frameworks. In: Proceedings of the 22nd International Symposium on Reliable Distributed Systems (2003)
8. Belqasmi, F., Glitho, R., Dssouli, R.: Ambient Network Composition. IEEE Network Magazine 22(4), 6–12 (2008)
9. Xiao, J., Boutaba, R.: QoS-Aware Service Composition in Large Scale Multi-domain Networks. IEEE Journal on Selected Areas in Communications 23(12), 2344–2360 (2005)

10. Johnsson, M., Schieder, A., Hancock, R., et al.: Final System Description. Public deliverable D18-A.4. Technical report, Ambient Networks project (2008)
11. Andres-Colas, J., et al.: Design of Composition Framework. Public deliverable D3-G.1, Ambient Networks project (2006)
12. Callejo, M.A., Zitterbart, M., et al.: Draft architecture framework. Public deliverable D-2.2, 4WARD project (January 2009)
13. Boudjemil, Z., Mulligan, T., Fahy, C., Finnegan, J., Dempsy, S.: Language and Open Metamodel for E-business Negotiations. In: Proceedings of Digital EcoSystems and Technologies Conference, DES 2008 (2008)
14. Telesca, L., Finnegan, J., Ferronato, P., Malone, P., Ricci, F., Stanoevska-Slabeva, K.: Open Negotiation Environment: An Open Source Self-Learning Decentralised Negotiation Framework for Digital Ecosystems. In: Proceedings of Digital EcoSystems and Technologies Conference (DEST 2007), pp. 186–191 (2007)
15. Singh, G., Buricea, I., Mao, Z.: Composition of Service Specifications. In: Proceedings of the Sixth International Conference on Network Protocols (1998)

Taxonomy for GP-Aware Mobility

Sérgio Figueiredo[1], Justino Lourenço[1,2,3], Rui Aguiar[1,4], and Augusto Neto[5]

[1] Instituto de Telecomunicações de Aveiro, 3810-193 Aveiro, Portugal
[2] Inst. Superior Politécnico Gaya, 4400-103 Santa Marinha - Vila Nova de Gaia, Portugal
[3] Universidade de Vigo, C.P. 36310 Vigo, Spain
[4] Universidade de Aveiro, 3810-193 Aveiro, Portugal
[5] Instituto de Informática, Universidade Federal de Goiás, Brazil
{sfigueiredo,jml,ruilaa)@av.it.pt, augusto@inf.ufg.br

Abstract. We present a structured analysis for classification of diverse mobility schemes, resulting in a taxonomy for mobility in Future Internet systems. The different approaches discussed are based on the Generic Path (GP) concept, a unified framework for the transport of information, and all of them revolve around the existence of a binding between the user and the end-to-end path. Each of the schemes is mappable to real existing and envisioned scenarios, and cover a broad type of services, such as conversational, streaming or interactive ones. As a base to this structured analysis, the work introduces the concept of Generic Path Management Record (GPMR), a flexible record capable of storing relevant information for any type of path, at any level, such as throughput, delay SNR or even authentication paramenters. Thereby, GPMR behaves as much more than a mobility tool, extending its usefulness to everything related to the Network Management universe.

Keywords: 4WARD[1], Future Internet, GP, GPMR, Mobility support.

1 Introduction

The evolution of the actual Internet is a major current concern in the Telecommunications field, with the all-mighty Internet model, supported by the TCP/IP stack, showing its age. This model was created considering simple information transfer, such as file transfer and messages, in-between a restricted number of trusted nodes interconnected by copper. Such simplistic vision became increasingly inadequate to evolving user needs, and some alternative patches to this became commonly discussed, such as IPv6 [2] MIPv6 [3] DCCP [4]or SCTP [5] Part of the issues raised by the integration of new protocols in the Internet are correlated with the experience of more and more complex scenarios, mainly due to heterogeneity. For instance, it is noted the increasing demand for video streaming sessions (e.g., IPTV) by group of users simultaneously. In such scenario, users (mobile or not and supporting different network interfaces) of the same group can be connected to different network technologies (Wi-Fi, WiMAX, 3G, etc.), as well as receive the data content through different transport schemes (broadcast, unicast and/or multicast). Thus, the simple Internet initial model has deeply changed in order to support set of new functionalities. Additionally, the

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 93–104, 2010.

end-to-end model has been questioned long ago: a simple HTTP session, originally intended for as an end-to-end transaction, is now frequently intercepted by firewalls and proxies along the path. As a matter of fact, in spite of the huge success of the current Internet architecture, it is clear that we are not facing the ideal solution since it does not fit the needs brought by such new elements as optical communications systems or the inclusion of mobility and security as guaranteed features. A new Internet framework should take into account aspects and questions like naming, addressing, routing, QoS, self-management, seamless mobility, reliability and availability, interoperability, scalability, security, power consumption optimization and performance enhancement. Heavy investment was put for researching the proper evolution for the Internet ([6][6], [7][7], [8][8]), with proposals alternating between the introduction of single-problem solutions, and the design of a clean slate architecture, both taking into consideration the foreseen services and characteristics that Future Internet should supply.

This work focuses in the ways mobility can be assured in future models. The attempt to add efficient mobility to the current Internet architecture is handicapped, in a great part due to the locator-identifier dependence, with current solutions for Internet naming based on the host address, typically the IP address. In order to provide routing scalability, the actual model uses a hierarchical method of addressing, which implies that the host address has an intrinsic relation with its location. Most works regarding this issue start out by breaking out the hierarchical routing scheme or by rebuilding the IP addressing, which in other words means the redefinition of the Internet structure itself. One of these approaches is the IST 7th Framework Programme Integrated Project 4WARD, which aims to combine the innovations needed to improve the operation of any single network architecture with the coexistence / interoperability of diverse and complementary network architectures in a unique framework. Inside 4WARD, the concept of GP [9] has been introduced [9], [10], which brings an abstract way of describing the transport of information between (two or more) communicating parties, whatever the type of communication is, and improving operational efficiency for both the user and network. As we discuss in Section 2, in order to support this framework, a new functional element is introduced, the GPMR, a record designed for storing all relevant information of the GP, such as QoS parameters and associated *End Points* (EPs). Taking into account that the GP can be defined at any communication level, the information that GPMR will store is distinct according to the corresponding GP level. This is a major characteristic that shows the relevance and usefulness, in particular for mobility support. In Section 3[11], we present a four elements taxonomy for mobility within GP architecture [11], and conclude the paper in Section 4.

2 The Generic Path Concept

Networks share a content delivery task between sources and destination nodes that may be linked by different types of physical technologies, with information traveling by traversing relay nodes that simply provide sub-paths. These sub-paths, when compounded, form the end-to-end path, built with the support of several layers.

Based on such reality, 4WARD approach brings the concept of Generic Path (GP) as an abstract form of information transport that can either represent a physical point-to-multipoint connection or the distributed information exchange between applications. For this to be feasible, the GP concept follows an object oriented approach, allowing its instantiation to benefit from class specific characteristics, well adapted to the aimed transport service. By definition, GPs start and end at EP*s*. A GP can have more than one source of information connected to more than one sink of information, in a multi-point to multi-point way, this way redefining the concept of end-to-end.

2.1 Generic Path Architecture Elements

In the proposed 4WARD Generic Path architecture several blocks were introduced and will be briefly described in this section.

A Generic Path is a means for transferring information between two or more End Points. An EP acts as the interface between the GP termination and the Entity (i.e., the client), and it uses an identifier, the EID (Endpoint Identifier). The bootstrap of a new GP is done by a functional component called GP Factory, which exists within each compartment (CT, described later).

Concerning the morphology, GPs can be defined to support point-to-point, point-to-multipoint or multipoint-to-multipoint connections between EPs.

The GP represents the connections between the same or different layers in a common way. In a top-down perspective, an end-to-end (E2E) GP (representing the overall path used in the connection) may for example be mapped at the physical level to a wireless channel (e.g. WiFi, WiMAX) or to a wavelength at an optical fiber (WDM). For example, considering a communication in a university campus, we can figure out the need for establishing a GP between two processes, each in a different terminal. At network level we can think of a single GP for the information dissemination mapping into a concatenation of several smaller GPs, at data link level, which at last are adequately mapped into physical channels (see Fig 1).

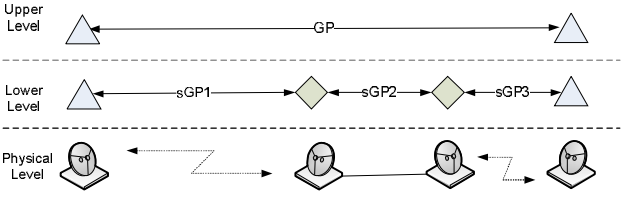


Fig. 1. Different GP levels mapping

Besides the ability to map and negotiate link properties, each GP is expected to efficiently react under unpredictable network dynamic events, so that the continuity of on-going transmissions with required QoS guarantees can be ensured. Examples of network dynamic events that endanger such transmissions are the radio conditions deterioration, load evolution and interface connectivity variations. In this sense, self-organization and resilience support is crucial, which must take into account performance issues in terms of scalability and optimized operations.

It is expected that the GP abstraction should deal in an efficient way with multiplicity of connectivity interfaces, from the same or different technology, in a simultaneous (multihoming) or sequential manner (handover). In order to assure mobility is handled efficiently, each GP should "react" to the various scenarios characteristics, by providing the necessary API to dynamically add and remove EP's.

The GPs are created and managed in a network block called *compartment*. Each *compartment* is associated to a specific administrative domain and a particular technology support, defined at any level. This implies the existence of (e.g.) IP, Ethernet and TCP *compartment*s, at different levels. Each GP branch will be the collected contribution of several sub-GPs branches linked within all the heterogeneous *compartment*s that the information needs to travel through to reach the sink(s). In Fig 2, we illustrate this GP concatenation process in different *compartment*s. The vertical compartments are called *Node Compartments*, and represent the processing system, or node.

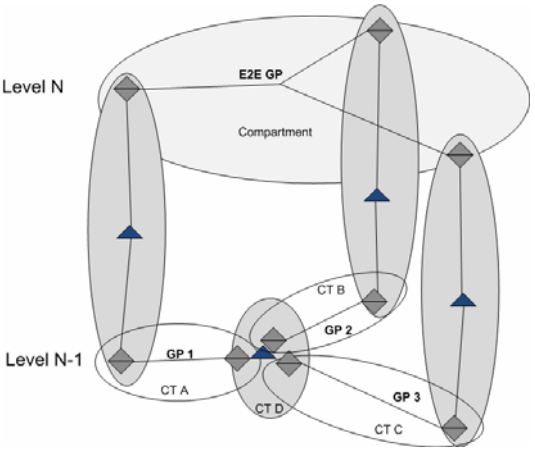


Fig. 2. GP existence within different levels

Mediation Points (MPs, triangles in blue) have the main purpose of interfacing different connections, by interconnecting EPs within the same CT, providing functions of buffering, multiplexing, transcoding and bit rate adaptability, assuring the information flow between distinct connections / GPs. For example, when a terminal moves out of range of the old base station, a branch of the GP could be torn down as the terminal no longer can communicate with the old base station – in that case the existence of mediation points in the base station seems like a valuable solution. To conclude, the MP has functionalities to "fork" GPs, that is, to discover and to set up alternative routing solutions to the same endpoint (e.g. multi-path routing mechanism is a possible mechanism for user mobility).

2.2 The GPMR Concept

In order to fulfill the end-to-end path requirements, such as connectivity (supported by multihoming, either with multiple interfaces or technologies), or the holy grail of

mobility, seamless handover, the GP architecture must provide efficient means for control and support. As the information derived from the creation of each GP needs to be acted upon, a way is needed for collecting and controlling this information. We propose the introduction of a record for storing relevant characteristics from each of the GPs within its local *compartment* – the GPMR - and another one for storing the E2E (across all *compartment*s) GP information – the Master Record (MR) a innovative solution relatively to nowadays networks that provides a unified framework about the communication path . As an abstraction, the GP depends on proper control, and as the element that stores all the information about the GP, GPMR can provide such feature.

The first issue to be tackled is the question "Where to locate the GPMR?" Several approaches were studied in our research. For the sake of brevity, we present the pros and cons of some alternate proposals considered for the GP record location (Table 1).

Table 1. GPMR Location Alternate Proposals

Location	Advantages	Disadvantages
At each Entity	Record is kept out of the network core	Entity heterogeneity compromises implementation simplification
At both EP's	Adds resilience to the network	Redundancy / Information replication/synchronization adds overhead
At the Source EP	Process simplification as only one element is responsible for each GP record; Source doesn't need to be concerned about network topology changes	EP needs to maintain a record; Mobility makes tracing of GP status difficult / impossible.

After evaluating aspects such as centralization and added value to path management, the best option seems to be placing the GPMR at each CT that the GP traverses, which results in multiple GPMRs "tracking" the same higher level GP. The advantages for such a solution include:

i. The decentralization of GP functionalities;
ii. Optimization in GP look-up operations;
iii. Technology and communication type independent (any type of GP can be described this way);
iv. A QoS aware element which allows relevant entities – Entities, GP Factory, In-Network Management (INM), etc - to trigger necessary routing / GP reconfiguration decisions;
v. Flexible solution that can be optimized for different mobility cases by simply varying the mobility indirections.

As for the disadvantages:

i. Considering very dynamic GPs: future studies must analyze scalability; how big can a CT be and how would the number of updates increase with it?
ii. From an end-to-end point of view, a MR is the result of the concatenation of various GPMRs, implying a large amount of information exchange.

Fig 3 shows a possible relationship between MR and the different GPMRs. A, B and C correspond to different node CTs, and each of the records is able to communicate with other records, as long as they're responsible for a common higher level GP. Additionally, a GPMR may talk to more than on MR, e.g., when more than one higher level GP are simultaneously using a lower level GP.

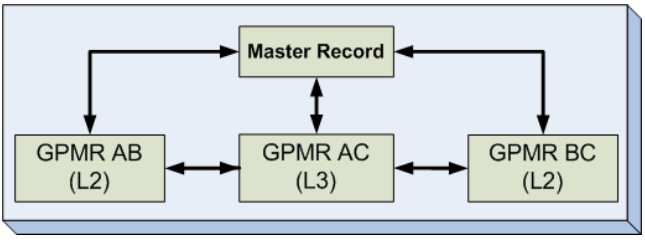


Fig. 3. MR Information Hierarchy

Fig 4 depicts the GPMR within a CT and the relationship with other functionalities. The GPMR is being defined to provide support for GP operations related to the GP factory, namely GP creation and destruction, and for later usage by mechanisms such as QoS-aware routing, traffic engineering, resilience, and so on. For instance, network management and control blocks should supply GPMR with up-to-date QoS-related information as a result of their network management and resource control operations. Available network control schemes must update QoS capabilities of a GP after setting up a bandwidth reservation along it, or periodically via soft-state operations. The same idea is also addressed for Traffic Engineering support.

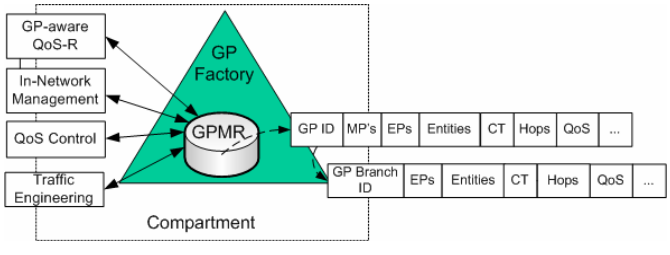


Fig. 4. GPMR Functionalities

Major issues about the GPMR and subject for future work include determining the amount of information that should be traded between GPMRs of different levels, a key aspect that must be well defined to better provide cross-layer optimization. A possible solution would be the module definition inside MR. Another problem is the GP architectural elements namespaces definitions, e.g. GP, EP. In future work, an analysis and enhancement of this solution by the introduction of Media Independent Handover (MIH) mechanisms is also intended. The IEEE 802.12 MIH standard [12] provides media independent mechanisms that aid and optimize the handover process, using commands and events to obtain information about different access technologies, enabling MIH-enhanced management entities to better select handover candidates.

Although these mechanisms are more oriented towards handover operation, information is itself an important part in the GP global architecture. MIH mechanisms can be introduced as the providers of such information (either dynamic through the Media Independent Event Service) or static (Media Independent Information Service) enabling GP Factories to establish paths based on optimum choice conditions (i.e., optimize route by choosing nodes with low load and that better support a specific kind of traffic such as VoIP, or updating a path due to foreseen out-of-range from a terminal's current signal strength analysis). Also relevant is what kind of information objects should be used, because MIH focuses on handovers while GP also involves all the necessary steps for data communication, such as routing and session establishment.

3 Mobility and Generic Paths

The work around the definition of Future Internet should take special concern on mobility. The typical network user will roam between several different technologies while moving, and will need transparent, fast and accurate handover support.

3.1 Mobility Types

Supporting wide scale mobility raises new issues. Current IP network architectures do not provide satisfactory solutions (see e.g. [3]) but an inefficient handling of mobility via add-on mechanisms. Some of the main Internet shortcomings include the lack of support for multi-homing, fast handover, simultaneous multi-access, and non-intermittent connectivity in wireless networks. Those important requirements work as core drivers to new designs for mobility support in the Generic Path architecture.

As a starting point in our work, we distinguished the different types of mobility: user mobility, session mobility and network mobility.

User mobility implies the change of the point of attachment that best serves the user by the network, assuming the simultaneous movement of the Entity residing in the terminal. Within this approach we can also state that the corresponding moving end-point will need to change, in order to build a GP that better fits the new geographical position of the device. There is also the case where there is no movement of the user, but for guaranteeing the QoS levels the user may detach from the current access point and connect to another.

Session mobility occurs when the user plans to move the service between terminals. This takes places when, e.g., a user is participating in a video-conference, and as soon as it gets to his office plans to migrate it to the desktop computer. In our architectural approach this means that the end point and the Entity must be moved from one terminal to another terminal. The transference of the session can be triggered by the user or by the network. In this process, some similar steps to the previous approach should be taken. The GP established for the video-conference should somehow be redirected to the desktop, and MP functionalities will aid in traffic redirection and video transcoding.

As for network mobility, we can think of a scenario where a network is established in a vehicle, implying constant mobility. In such case, the GPs defined between the network nodes should be more or less static, except the ones connecting the vehicle to the outside network.

3.2 Mobility Taxonomy

In order to provide the desirable mobility in the future Internet, several scenarios have been conceptually studied. As previously described the GP will be responsible for the flow of the information between the communications entities, so, as long as the endpoints have some sort of mobility, it will be necessary to develop a strategy for the handover mechanism and to maintain the communication with the desirable QoS parameters. Four different scenarios aiming to fulfill the requirements have been identified, with potential realizations in different CTs.

Dynamic GP Modification

The first approach, *Dynamic GP Modification*, is based in the constant GP updating each time that any kind of mobility occurs, fitting the overall concept of a *moving GP*. It can be stated that the GP becomes a lively entity, constantly being created, destroyed and modified in association to the physical realization. Such a GP vision grants that all GPs are fully flexible and dynamic in terms of behavior.

In the example of Fig 5, EP 1 communicates with EP 2 by means of an intermediary MP, for example due to physical distance. The trajectory that EP 1 did allowed it to become closer to EP 2, which in terms of GP modification, possibly by soft handover represented the following: i) creation of GP 3 and respective introduction into the CT GPMR, in an entry parallel to GP 1 + GP 2, as it represents a E2E GP with common EPs; ii) sequential destruction of GP 1 and GP 2, and removal from GPMR. Regarding routing processes, as communication is done directly between the EPs, no routing / forwarding is now needed as before through the intermediary MP. Nevertheless, special concerns should be taken when adopting this method, due to the inherent delay in the creation / destruction of each new GP branch: problems associated with the synchronization and replication at the endpoints should be taken into account.

Concluding, this scenario involves fast and accurate creation and destruction of GP branches (e.g. GPs at a given CT), translating into a constant update of the GPMR, mostly at the data link and network levels, and in complex manageability when considering high mobility networks. This solution provides a simple and uniform scheme independently of the type of communications established, and could be optimally used in small or low mobility, for example in backbone and at the core of the network.

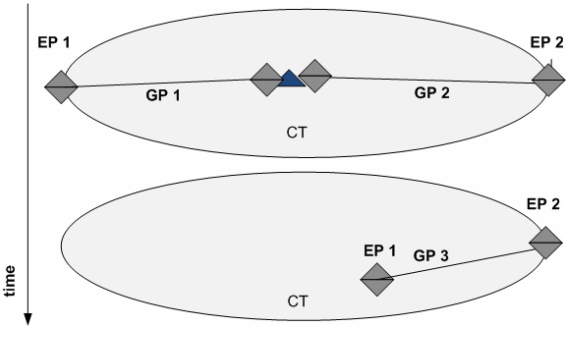


Fig. 5. Dynamic GP Modification Representation

Continuous Binding Scheme

The second proposed solution is the *Continuous Binding Strategy*, where each GP is composed of two parts, each of them characterized by the associated EP type. The use of different kinds of EPs by a GP was first presented in Anchorless Mobility approach [14]. We can state that this scheme is centered on the EP binding function. In its most basic design, a connectivity EP detaches from a locator EP and binds to the next available locator EP. GP is physically reconfigured, maintaining the communication between entities. This implies that the GP is actually built from two parts, one between locators EPs (or MPs), and the other between the connectivity and logical EPs, as shown in Fig 6.

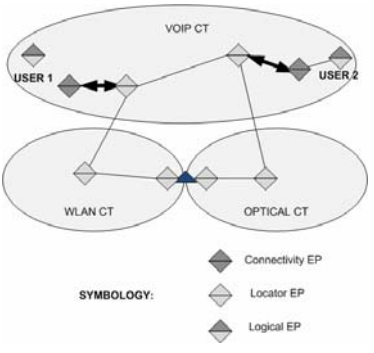


Fig. 6. Continuous binding scheme representation

Static Multiconnection P2MP

The third proposed solution is the *Static Multiconnection P2MP GP,* which assures strong mobility coverage without the need for a binding function. Such mobility solution is targeting wireless technologies, and is possible mostly at the physical level, as the main decision factor is the physical coverage area, measured in terms of transmission power. We propose the creation of a point-to-multipoint GP that assures persistent coverage of the user whatever its current geographic position is (Fig 7). This level of connectivity is supported not only by its coverage cell, but also by the neighbor cells.

As advantages, we can refer the reduced amount of mechanisms needed for small mobility scenarios, avoiding the delay inherent to the constant creation, destruction or changing in the GP that assures the communication. That is also a consequence in terms of low GPMR amount of updating. We also avoid the disadvantages of supporting binding functions. On the other side, it brings a traffic increment because of the need for broadcasting, as the same data flow is sent to the user and to all the other network points on its vicinity.

As solutions that are included in this scheme, we can immediately think of a swarm scenario, and other P2MP or MP2MP schemes, as the newly proposed Concurrent Multipath Transfer [14].

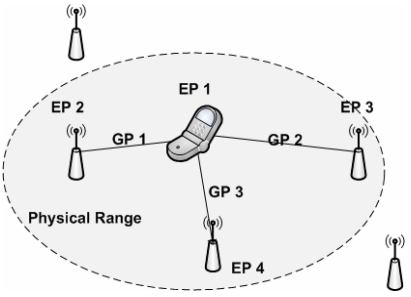


Fig. 7. Static multiconnection P2MP example

EP as an Anchor

As a last solution, we present the EP as a simple Anchor. In this approach we use the concept of anchoring, as the EP can be considered as an anchor that serves a particular geographical area. So as long as the user moves in between this area, the anchor serves as data flow supplier to all the network access points.

In Fig 8, EP 1 is communicating with both EP 2 and EP 3. As can be seen, all traffic towards EP 1 is handled by the Anchor EP, as long as EP 1 is within the anchor range. In the moment that EP 1 leaves this range, a new Anchor EP is obtained, either by EP 1 or by the actual anchor EP request.

This last solution provides simplicity and also avoids the concern about the mobility of the GP restrained to the mobility of the user. However, in this scheme it is necessary to gather information about macroscopic localization of the user, as well as controlling the data flow as soon as the user leaves the anchor coverage zone. In terms of GPMR, the level of updating varies depending on the level in which the GPMR applies; the level of updating is null when the mobility is within the anchor range, avoiding considerable overhead. Solutions that can be integrated in this scheme are the already proposed hierarchical mobility schemes and also an innovative scheme, Dynamic Mobility Anchoring [14] proposed within 4WARD project.

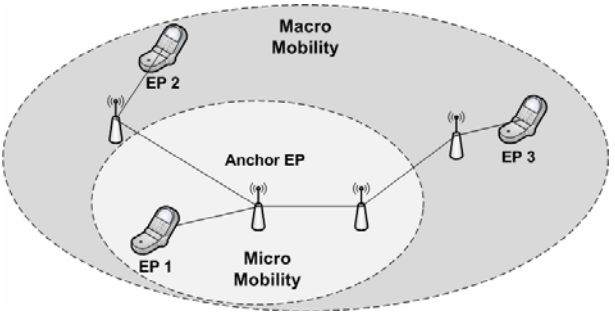


Fig. 8. EP as an anchor example

3.3 Paradigms Comparison

This section provides a resume of each of the mobility schemes in terms of some of the most relevant properties, such as flexibility or scalability. Naturally, these models will be associated with the specific technology realization, and its inherent constrains.

Table 2. Comparison mobility models for GP architecture

	Dynamic GP Modification	Continuous Binding Scheme	Static Multiconnection P2MP	EP as an Anchor
Flexibility	High	High	Average	High
Delay associated to operations	Depends on level of mobility	Average	Low	Low
Scalability	Average	Average	Large	Large
Connectivity Strength	Average	Average	High	Average

4 Conclusions and Future Work

This paper started describing the clean-slate approach brought by the Generic Path concept for the future Internet. We have introduced in a brief manner the architectural elements related to the GP approach and its importance in mobility. The GPMR concept was originally proposed as a solution for keeping a record about the state of a GP, providing a powerful tool for being used in mobility scenarios. Regarding the usage of MIH mechanisms it is still unclear at this point in time the best way to integrate MIH into our GP architecture, due different objectives of both approaches and due to the GP as a still evolving solution. We are currently evaluating how to best apply 802.21 functionality to GP boxes and how to adapt MIH-alike behavior into GP concepts.

We presented several models for the types of mobility for Future Internet under the scope of the GP architecture, obtaining the most relevant solutions, with each of them comprising a broad range of mobility scenarios and mapping to more concrete cases.

Our current research is aiming to evaluate and compare those different approaches with real technologies and how they could coexist, in order to provide the best approach for dealing with the mobility issues for the future Internet definition in the 4WARD Project.

Acknowledgments

We would like to thank our colleagues in the 4WARD Work Package 5, aptly titled Generic Paths, for fruitful discussions, in particular to our research group at IT-Aveiro. Special thanks go to Eng.. Daniel Corujo, who shared with us an interesting view on a possible interaction between MIH and GP architecture.

This work has been carried out in the framework of the IST 7th Framework Programme Integrated Project 4WARD, which is partially funded by the Commission of the European Union. The views expressed in this paper are solely those of the authors

and do not necessarily represent the views of their employers, the 4WARD project, or the Commission of the European Union.

References

[1] The FP7 4WARD Project, http://www.4ward-project.eu/
[2] Johnson, D., Perkins, C., Arkko, J.: IP Mobility Support in IPv6, RFC3775, IETF (June 2004)
[3] Soliman, H., et al.: Hierarchical Mobile IPv6 Mobility Management (HMIPv6). rfc4140.txt, IETF (August 2005)
[4] Floyd, S., Kohler, E.: Profile for Datagram Congestion Control Protocol (DCCP) Congestion Control ID 2: TCP-like Congestion Control. RFC 4341, Internet Engineering Task Force (March 2006)
[5] Stewart, R., Metz, C.: SCTP: new transport protocol for TCP/IP, Internet Computing. IEEE, Los Alamitos (2001)
[6] Siekkinen, M., Goebel, V., Plagemann, T., Skevik, K.A., Banfield, M., Brusic, I.: Beyond the Future Internet–Requirements of Autonomic Networking Architectures to Address Long Term Future Networking Challenges. In: 11th IEEE International Workshop on FTDCS (March 2007)
[7] Gavras, A., Karila, A., Fdida, S., May, M., Potts, M.: Hierarchical Broadcasting in the Future Mobile Internet 37(3) (July 2007)
[8] Wong, W., Villaca, R., de Paula, L.B., Pasquini, R., Verdi, F.L., Magalhaes, M.F.: An Architecture for Mobility Support in a Next-Generation Internet. In: AINA 2008 (March 2008)
[9] Guillemin, F., Woesner, H.: Path Generalizations in a Functional Architecture. In: ICT, Mobile Summit 2008, Stockholm (2008)
[10] Guillemin, F.: Architecture of a Generic Path, 4WARD Deliverable D5.1 (2008)
[11] Söllner, M., et al.: Mobility Scenarios for the Future Internet: the 4WARD Approach. In: WPMC 2008 (2008)
[12] IEEE 802.21 Standard, Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services (January 2009)
[13] Matos, A., Aguiar, R.L.: Mobility Aware Paths: The Identity Connection. In: WPMC 2008 (2008)
[14] Bertin, P., Aguiar, R.L., Folke, M., Schefczik, P., Zhang, X.: Paths to Mobility Support in Future Internet. In: ICT 2009 (2009)

Session 4:
Wireless Networking

Topology-Aware Hybrid Random Walk Protocols for Wireless Multihop Networks

Vasileios Karyotis[1], Fabio Pittalà[2], Maria Fazio[2], Symeon Papavassiliou[1], and Antonio Puliafito[2]

[1] Institute of Communications and Computer Systems (ICCS)
National Technical University of Athens (NTUA)
School of Electrical and Computer Engineering
Zografou, 15780, Athens, Greece
vassilis@netmode.ntua.gr, papavass@mail.ntua.gr
[2] University of Messina
Faculty of Engineering
Contrada Papardo, S. Sperone, 98166, Messina, Italy
fabio.pittala@estudiante.uam.es, mfazio@unime.it, apuliafito@unime.it

Abstract. The proliferation of wireless multihop networks has made various operations, such as search and retrieval of distributed data a significant concern. Various methods have been proposed for performing such tasks efficiently, especially when all network nodes need to be visited at least once. Random walks are probabilistic approaches for performing the aforementioned operations effectively and with relatively small overhead compared to other typically-employed schemes, such as flooding. Recently, a hybrid random walk scheme has been proposed for increasing the desired performance, at the cost of additional consumed resources. In this work, we adopt the paradigm of hybrid random walk protocols and propose two novel hybrid schemes that exploit local topological information, aiming at further increasing the performance of random walk protocols in multihop networks. We consider different jump configurations of the hybrid random walk protocols and various degrees of mobility. Through analysis and simulation, the simple random walk model appears more appropriate for energy-constrained networks such as sensor networks, while the hybrid ones are more appealing for less energy-stringent, performance-oriented multihop networks, such as vehicular and mesh networks. The simple hybrid protocol occupies the middle ground, being appealing for ad hoc networks with medium to low node densities and average energy requirements.

Keywords: hybrid random walks, topology awareness, mobile multihop networks.

1 Introduction

Wireless networks can potentially have large sizes, in terms of the population and/or the deployment region they span. In addition, most of these networks,

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 107–118, 2010.

like ad hoc, sensor, mesh and vehicular, are of multihop nature and they are characterized by lack of central infrastructure and dynamic topology. Search in these networks can be rather costly, especially in cases where all network nodes need to be visited at least once, or visited only once, as it is required in the famous Traveling Salesman Problem (TSP) [1].

Various approaches have been proposed for performing search, dissemination and retrieval in large unstructured networks and visiting all nodes of graphs representing such communication networks. Flooding schemes have been used extensively for their optimal performance [2,3]. However, such schemes suffer from the packet explosion problem, which can be critical for the operation of energy-restricted networks. Alternative methods with comparable performance but significantly less overhead have been devised, most notably the probabilistic random walk [4,5]. Random walks operate in a state-less fashion requiring only locally available information for their operation.

Random walks have been employed in diverse network types and applications, mainly for performing query search, network sampling and sensor data collection/spreading. In [4] the effectiveness of random walks for searching/construction of Peer-to-Peer (P2P) networks is analyzed. In the considered framework, random walks achieve improvements over flooding for searching applications in two practical cases, namely in clustered P2P networks and when the same query is re-issued multiple times. In [5], it is shown that the coverage time (i.e. time to visit all network nodes at least once) for a random walk with look-ahead in a power-law graph (frequently used to represent the network graph of autonomous systems (ASs) of the Internet) is sublinear. In [6], constrained and unconstrained random walks over square lattices of sensor networks are studied and a closed-form expression for coverage in unconstrained random walks over the square lattice is obtained. Within this framework and available analytical expression, an optimal lattice form is conjectured and proposed. It is also concluded that constraints on random walks increase their efficiency. In [7] different types of random walks are studied for random graphs, a model commonly used for representing social and other topology-evolving networks.

In our work, we focus on hybrid random walk schemes in wireless multihop networks, where nodes perform either single or multiple hop jumps in successive steps of the walk. The main idea is inspired by [8], in which a two-state Markov chain is employed for performing multihop jumps or single hop visits. The proposed scheme achieves fewer node revisits and in general it is found that longer average jump lengths lead to higher performance at the expense of increased energy consumption. We propose two novel hybrid random walk protocols that attempt to improve the performance of the walk by exploiting local topological information. We then compare the performance of these protocols with that of the basic hybrid random walk protocol and the typical random walk, in order to obtain the most appropriate technique for different network application scenarios.

The rest of the paper is structured as follows. In section 2 the network model and random walk framework are described, while in section 3 the adopted and

proposed hybrid random walk protocols are presented and analyzed. In section 4 comparative numerical results are presented and based on them conclusions are drawn on the suitability of each protocol for the considered networks and application environments.

2 Random Walk Framework

In this work, we consider a wireless, mobile, multihop network consisting of a set $V = \{1, ..., N\}$ of N nodes. The network can be modeled as a graph $G = G(V, E)$, where E is the set of links representing reliable wireless channels between communicating nodes. Without loss of generality, each node is considered to have the same initial available energy reserves E_{init}, transmission power P and corresponding transmission radius R. A deterministic wireless channel, in which the receipt power decays with respect to a specific power of the distance between the transmitter-receiver is considered (the decay factor being the path loss constant γ). Thus, for deterministic channel conditions, two nodes are considered neighbors if each one lies within the other's transmission range. Nodes are initially randomly and uniformly deployed in a planar region, which is considered to be square of size A. Essentially, the considered network model is a Random Geometric Graph (RGG) [9] in two dimensions.

The adopted graph model is able to accurately represent any type of wireless multihop networks, like ad hoc, sensor, mesh or vehicular. In Table 1 we summarize the macroscopic features of such networks according to the parameters of node density, network size, degree of mobility and energy constraints. Variations of such characteristics, that however do not significantly affect the generality of the analysis, may be identified in several cases.

In probability theory a Random Walk (RW) is a Markov process $\{X_i\}_{i \geq 0}$ in which X_i denotes the state of the process at step i and the next state is randomly and uniformly chosen among all the possible next states of the process.

Table 1. Wireless multihop networks' features

	node density	**network size**	**degree of mobility**	**energy constraints**
ad hoc networks	low/medium	small/medium	medium	medium
sensor networks	high	medium	none/low	high
mesh networks	medium	large	none/low	none
vehicular networks	medium/high	large	high	none

In our study the objective of the walk is to visit all network nodes at least once in some sequential random order. An accurate representation of the visiting process is for the state of the walk to denote the vertex of the graph visited in each time step, so that in the i-th step of the walk $X_i = v$, $v \in V$ being the label of the currently visited node. In the basic version of a RW on a network graph, transitions are allowed only between neighboring nodes. Each neighbor is chosen with equal probability. In this work we refer to the plain version of a RW as Simple Random Walk (SRW). If d_v denotes the degree of node $v \in V$, then the transition probabilities between states (i.e. neighboring vertices) are $P_{u,v} = \begin{cases} \frac{1}{d_u} & \text{if } (u,v) \in E \\ 0 & \text{if } (u,v) \notin E \end{cases}$ and the stationary probabilities, i.e. the probability for the walk to be in state u is $\pi_u = \frac{d_u}{2|E|}$.

Several quantities of interest may be defined for the SRW. In this paper we will focus on the expected number of steps required to visit all network nodes at least once, denoted by the term Cover (Coverage) Time, C. We also take into account the number of revisits before all nodes are covered, used to acquire the total energy required to cover the network.

SRWs have been used extensively in wireless sensor networks, P2P and ad hoc networks for performing the aforementioned tasks with simplicity, exploiting locality of computation and at the same time provide increased robustness to failure [4,5,6,7]. Owe to their stateless fashion, mobility-induced topology and channel variations do not significantly affect (if at all) RW operation, as the only information required is locally available at the current state-node.

3 Hybrid Random Walk Protocols

In this section we present analytically the adopted and proposed hybrid Random Walk protocols for wireless multihop networks. Each of the proposed three strategies performs either simple one-hop jumps, or multihop jumps, the latter implemented as a sequence of one-hop jumps. For instance, if the random walk is currently at node 4 in Fig. 1 and performs a one-hop jump it can potentially transition to nodes $\{1,2,3,5\}$. However, if it performs three-hop jumps it will transition to node 7. In the latter case, the walk will pass through nodes 5 and 6 in order to visit 7. However this passage is not counted as visits of nodes 5 and 6 because such visits were not decided by the walk in this step. Nevertheless, the consumption for intermediate links needs to be accounted for, since it represents actual transmissions taking place.

More formally put, the walk constitutes a permutation of the set of node labels $V = \{1, 2, \ldots, N\}$ (visit sequence) determined by the specific protocol and network topology. In the case of SRW, the permutation is determined by the uniform distribution. On the contrary, in the event of a long jump in hybrid RWs, the permutation is decided by the nodes residing that many hops away as the length of the jump. The hybrid protocols aspire to improve the performance of the process by deciding proper sequences that yield small Cover Times. However, this happens at the cost of increased energy consumption, since a single

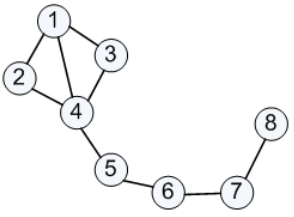


Fig. 1. Example of protocol operation

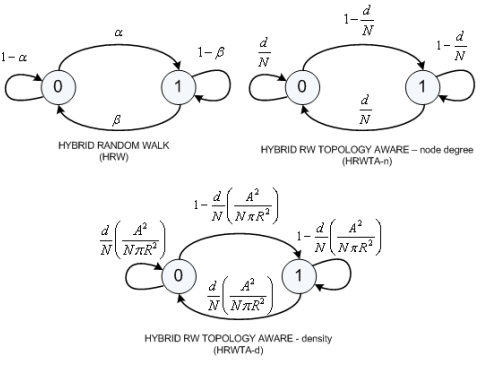


Fig. 2. Markov chains of the Hybrid Random Walk protocols

visit might require more than one transmission. Clearly, there exists a tradeoff between performance and consumption that the hybrid protocols need to balance. The main focus of this study is to specifically quantify this tradeoff and utilize it according to the application network.

3.1 Simple Hybrid Random Walk Protocol (SHRW)

In Simple Hybrid Random Walk protocol with parameters α, β, denoted by SHRW(α, β) [8], the random walk process has two states. When in state 0 (Fig. 2), the walk operates as a simple random walk, performing one-hop jumps out of each node it currently visits. When the walk is in state 1, it proceeds with multihop jumps. The multihop jumps in state 1 can be of fixed or variable length. In the latter case, the jump length is a random number uniformly distributed in the interval $[2, \ell_{\max}]$, where $\ell_{\max}$ is the maximum allowable jump length in hops. For compatibility purposes, $\ell_{\max} \leq D$, where D is the diameter of the network graph. In this work and in order to demonstrate the operation of the protocols in a simple way, we employ the uniform distribution for selecting the jump length. The direction of the jumps can be selected in various ways, and we choose again the uniform distribution direction among the available outgoing edges of a node.

The state transition probabilities of SHRW(α, β) are deterministic and remain fixed for the duration of the walk. More specifically, if at state 0, the process

switches to state 1 with probability α and remains in state 0 with probability $1-\alpha$. Similarly, when the process is at state 1, it transitions to state 0 with probability β and remains in state 1 with probability $1-\beta$ (Fig. 2). State changes (if decided) take place at each step of the walk.

As it will be demonstrated by the numerical results, the addition of long jumps to the conventional operation of SRW is expected to improve performance with respect to Cover Time. The intuition behind this is that long jumps potentially avoid local revisits caused in highly clustered areas of a multihop network. Furthermore, several spatially distinct nodes are covered quickly by means of the long jumps.

3.2 Hybrid Random Walk Topology Aware Protocol-Node Degree (HRWTA-n)

Hybrid Random Walk Topology Aware-node degree (HRWTA-n) works similarly to SHRW(α, β), but state transitions are now functions of the node degree of the currently visited node. More specifically, the normalized degree (node degree over the total number of network nodes, $\frac{d}{N}$) of the specific node is used as a transition probability. With probability $\frac{d}{N}$ the walk remains in the state with one-hop jumps, i.e. state 0, and with probability $1-\frac{d}{N}$ it transitions to the state with multihop jumps, i.e. state 1. On the contrary, if at state 1, HRWTA-n transitions to state 0 with probability $\frac{d}{N}$ and remains in state 1 with probability $1-\frac{d}{N}$ (Fig. 2).

The intuition behind the HRWTA-n scheme is that if the currently visited node has large node degree, i.e. large number of neighbors or equivalently large $\frac{d}{N}$, then it is more efficient to spent some steps of the walk in this neighborhood utilizing one-hop jumps in order to cover as many nodes as possible. On the contrary, if the ratio $\frac{d}{N}$ is small, i.e. the node degree is small, it will be more convenient to perform a long jump and move to a different neighborhood that it is not potentially already visited.

3.3 Hybrid Random Walk Topology Aware Protocol-Density (HRWTA-d)

The Hybrid Random Walk Topology Aware-density (HRWTA-d) protocol is similar to HRWTA-n. The state transition probabilities depend again on the topological information available at the node. Each currently visited node is able to measure the local density by dividing its node degree by its nominal coverage transmission area $\frac{d}{\pi R^2}$. The local density can be divided by the total network density $\frac{N}{A^2}$, since both the total number of nodes and coverage area are known to the nodes (design parameters). Division of the two densities yields the normalized local node density. Direct employment of this quantity was found to yield very abrupt transition probabilities, i.e. the transitions were very biased towards one of the two states. For this reason the normalized local density is multiplied by a scaling factor, that depends on the total number of nodes $K = K(N)$. In this work, we employ the factor $K(N) = \frac{1}{N}$.

Combining the aforementioned quantities the state transition probabilities from state 0 will be $\frac{d}{N}\left(\frac{A^2}{N\pi R^2}\right)$ for staying in state 0 and $1-\frac{d}{N}\left(\frac{A^2}{N\pi R^2}\right)$ for transiting out of state 0. On the contrary, the latter is the probability to remain in state 1 if already there and the first is the probability to transition to state 0 if in state 1 already (Fig. 2).

4 Numerical Results

In this section we present and discuss some results on the performance of the presented protocols, SHRW, HRWTA-n and HRWTA-d and SRW under several working conditions. The analysis has been performed through a simulative study, by implementing our own simulator in the MATLAB environment. Simulation scenarios have been built with the following settings: the network area was considered as an $A \times A$ square, with $A = 1000m$. Over this area, $N \in [100, 250]$ nodes were deployed according to a uniform distribution, which allowed the study of protocol behavior for increasing node densities. For simplicity, in Table 2 we summarize all the settings used in simulations.

Table 2. Simulation settings

Network size	$A = 1000m$
One-hop transmission power	$P = 1mWatt$
SHRW parameters	$\alpha = 0.3$ and $\beta = 0.7$
Communication range	$R = 150m$
Fix length jumps	$FixJump = 3$
Variable length jumps	$MaxJump = 5$
Low mobility	$Speed = [0; 2]$, $PauseTime = [0; 10]$
Medium mobility	$Speed = [0; 4]$, $PauseTime = [0; 7]$
High mobility	$Speed = [0; 8]$, $PauseTime = [0; 4]$

Multihop jumps in the network have been implemented in two ways: 1) fixed-length jumps, 2) variable-length jumps. We denote the first variation for hybrid modes of RW protocols with jumps by the term FixJump. In our simulations FixJump is set to 3 hops. The second variation is characterized by the MaxJump ($\ell_{\max}$) parameter, so that the length of each jump in hops, when the protocol operates in the multihop jump mode (state 1), is determined uniformly and randomly in the range $[2, MaxJump]$.

We have focused the analysis on two metrics:

- Coverage Time: the Coverage Time of a graph G is the expected time taken by a RW protocol to visit all the nodes in G. In this work, the Coverage Time is estimated as the number of steps in the Markov process.
- Energy consumption: the energy expended to visit all the nodes in G. The energy consumption model was taken as a simplified one, able to bind the

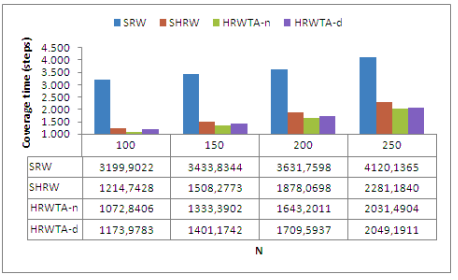
transmission power to the length of jumps. For one-hop communications, the transmitter node was assumed to spend 1 mWatt. Thus, if the protocol works in State 0, the power consumed was 1 mWatt. The power spent from a transmitter to make a jump was equal to the total length of the jump converted in mWatts.

Simulations have been carried out in two stages: at first, we have considered static nodes in order to understand the impact of jumps on the system behavior. Then we have repeated the experiments adding node mobility features, until all nodes are covered again. To provide informative and accurate results, all the simulation measurements have been averaged over 10000 different network topologies for each type of scenario.

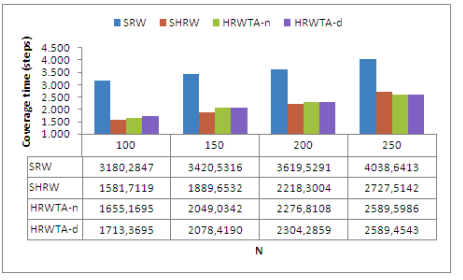
4.1 Analysis of Static Environments

In Fig. 3, we show the various protocol performances with respect to the Coverage Time for static scenarios. We distinguish performances of protocols for the MaxJump and the FixJump configurations. SRW exhibits the worst behavior, exemplifying the importance of jumps in providing desired networking service. By considering simulations with the MaxJump configuration, HRWTA-n presents better results followed by HRWTA-d and SHRW, but the gap in performance among protocols with jumps is narrow. In fact, the gap between HRWTA-n and SHRW is about 12% in all the network scenarios, whereas the gap between HRWTA-n and HRWTA-d depends on the nodes' density. In particular, it ranges from 8% for networks with low density of nodes ($N = 100$) to 1% in networks with high density of nodes ($N = 250$). The transition from the MaxJump configuration to the FixJump configuration results to protocols' performances degradation of about 37%, with a peak of 46% when N is small. In this context, the best protocol is SHRW when the density of nodes is low, while HRWTA-n and HRWTA-d perform better otherwise.

Results on protocol performances with reference to energy consumption are shown in Fig. 4. Simulations show that SRW and SHRW exhibit the best performances in terms of energy consumption. In particular, SRW carries out one-hop communications, thus minimizing the energy consumption for each data transmission. However, the low energy consumption for transmission is at the cost of high Coverage Time. On the contrary, HRWTA-n and HRWTA-d waste a lot of energy due to jumps. This is confirmed by the results on the time spent in State 1 for SHRW, HRWTA-n and HRWTA-d. In fact, nodes that run SHRW spend 30% of time in state 1 against the percentage of 90% if they run HRWTA-n and the percentage of 99% if they run HRWTA-d. The performances of SRW and SHRW are almost identical in dense networks, especially with regard to the FixJump configuration. SHRW performs better than SRW in large networks with low node density. When the density of nodes becomes high, SRW outperforms SHRW. Between HRWTA-n and HRWTA-d, the first always shows a better behavior in terms of energy consumption than the second. The best performances in terms of energy consumption are always under the MaxJump configuration,

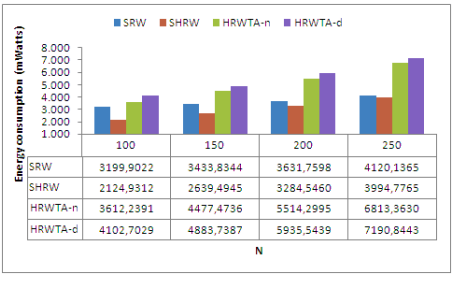


(a) MaxJump configuration

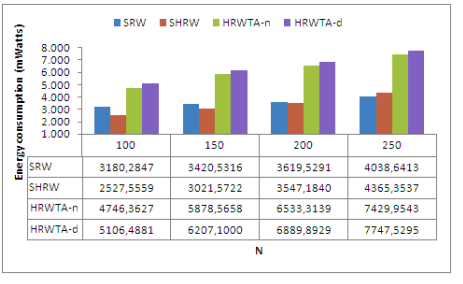


(b) FixJump configuration

Fig. 3. Coverage time in static scenarios



(a) MaxJump configuration



(b) FixJump configuration

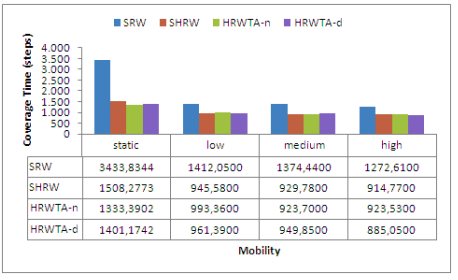
Fig. 4. Energy consumption in static scenarios

with a gap in performances between the two types of configuration in the range of 10-30%. In fact, long jumps reduce the coverage time and, hence, the number of transmissions in the network.

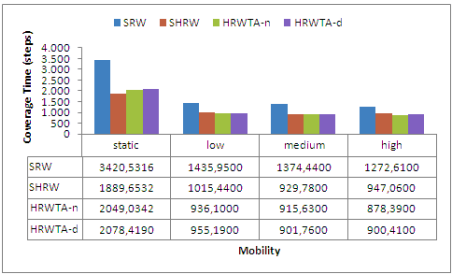
From previous considerations, we can assert that jumps in the RW protocols offer great benefits in the network delivery service. In fact, when we consider the Coverage Time as evaluation metric, protocols with jumps provide improvements of about 60% in the MaxJump configuration and 40% in the FixJump configuration over the SRW performances. Employing protocols like SHRW, HRWTA-n and HRWTA-d, takes place at the cost of higher energy consumption as opposed to the case of SRW. So, in wireless multihop scenarios where energy consumption is not an issue, like wire-powered mesh networks, HRWTA-n can offer the maximum efficiency in the networking services. On the contrary, SHRW is suitable in scenarios where nodes are limited in energy supply, like in sensor networks, since it guarantees a better Coverage service than SRW, but with significantly lower energy consumptions than hybrid protocols.

4.2 Analysis of Mobile Environments

In our simulation scenarios, node mobility has been implemented according to the Random Waypoint (RWP) model [10]. Nodes change their spatial

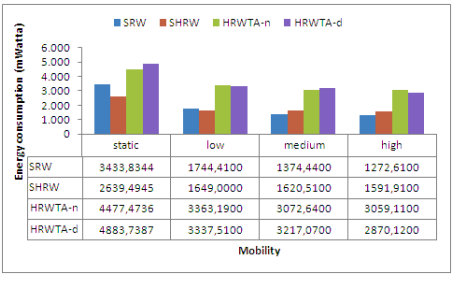


(a) MaxJump configuration

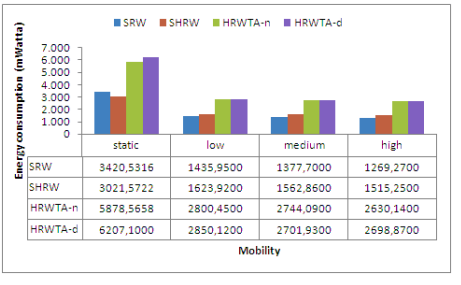


(b) FixJump configuration

Fig. 5. Coverage time in mobile scenarios



(a) MaxJump configuration



(b) FixJump configuration

Fig. 6. Energy consumption in mobile scenarios

distribution by uniformly and randomly selecting in the network area a destination trip (waypoint). Then, the trip path of a node is a straight line that connects the current node position with the trip destination. Also we have used three mobility degrees: low, medium and high to test protocols under different mobility conditions. Settings regarding the mobility degrees employed are provided in Table 2.

Mobility amplifies the effect of reducing local revisits of nodes, which is effectively, similar in concept to the execution of multihop jumps (different operation, similar outcome). A mobile node changes locations constantly, joining new neighbors and thus increasing the probability to visit uncovered nodes. By intuition, mobility can be considered as a different way to implement jumps in the network. This explains the improvement in the performances of all the protocols when we consider mobility in the network, especially of SRW that was not employing jumps previously.

In Fig. 5 and 6 we show experimental measurements on protocol performances by increasing the mobility degree and setting $N = 150$ for MaxJump and FixJump configurations. In general, the performances are always better in mobile scenarios than their counterparts in the static case both for Coverage Time and energy consumption metrics. Also, increasing the mobility degree, the overall performances increase. The protocol that mostly benefits from mobility

in terms of Coverage Time is SRW, since it does not implement any mechanism to avoid local loops and mobility helps in exactly this direction. In particular, it improves its performances by approximately 60%. Protocols with jumps also improve their performances, even at lower degrees than SRW. With reference to Coverage Time, gains of 33% in performances are achieved with MaxJump and of 56% with FixJump configurations respectively. Also, in both configurations, the protocols show very similar behaviors. Regarding the energy consumption metric, the improvement in performance with MaxJump is 36% and with FixJump 53%. Thus, the FixJump configuration allows to draw much more benefits from mobility. Even if SHRW shows the best performances among protocols with jumps, differences diminish by increasing mobility.

4.3 Discussion

In this subsection, we perform an overall assessment of the analyzed protocols. As mentioned earlier, both variations of HRWTA protocols have better performance but higher energy consumption. Consequently, they are more appealing for mesh and vehicular networks, where minimal energy requirements exist, if any. Furthermore, these networks have large sizes and medium to high node densities, calling for increased performance. Mobility degrees vary from very low (mesh) to very high (vehicular), however, the protocol operation will remain satisfactory, as it can only increase in the presence of mobility. Between the two, HRWTA-n is more suitable for vehicular networks and HRWTA-d for mesh networks, as HRWTA-n has a slightly better performance and respective increased consumption.

On the other hand, SRW and SHRW are more appropriate for ad hoc and sensor networks, due to their energy-conserving nature. Between the two, SHRW is more oriented towards medium to low densities, while SRW towards higher densities, in the sense that their performance gap closes towards these density extremes for each case respectively. Consequently, SHRW are better suited to ad hoc networks and SRW to sensor networks. Their energy-consumption fits ideally the corresponding network types, while for the indicated density ranges, their performance will not be significantly lower than the best-performing protocols.

Overall, hybrid protocols are more appropriate for performance oriented networks, while simple RW protocols for more energy-stringent. With respect to the protocols studied in this work, HRWTA-n is suitable for vehicular networks, HRWTA-d for mesh networks, SHRW for ad hoc and SRW for sensor networks.

Acknowledgment

The work of V. Karyotis was partially supported by Greek General Secretariat for Research and Technology of the Ministry of Development (PENED project 03ED840) by 25% and the European Social Fund by 75%.

References

1. Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: Introduction to Algorithms. The MIT Press, Cambridge (2001)
2. Stauffer, A., Barbosa, V.: Probabilistic Heuristics for Disseminating Information in Networks. IEEE Trans. on Netw. 15(2), 425–435 (2007)
3. Chang, N., Liu, M.: Controlled Flooding Search in a Large Network. IEEE Trans. on Netw. 15(2), 436–449 (2007)
4. Gkantsidis, C., Mihail, M., Saberi, A.: Random Walks in Peer-to-Peer Networks. In: Proc. of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), March 2004, vol. 1, pp. 120–130 (2004)
5. Mihail, M., Saberi, A., Tetali, P.: Random Walks with Lookahead in Power Law Random Graphs. Internet Math. 3(2), 147–152 (2006)
6. Lima, L., Barros, J.: Random Walks on Sensor Networks. In: Proc. of the 5th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt), Limassol, Cyprus, April 2007, pp. 1–5 (2007)
7. Dhillon, S.S., Van Mieghem, P.: Comparison of Random Walk Strategies for Ad Hoc Networks. In: Proc. of the 6th IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), Corfu, Greece, June 2007, pp. 196–203 (2007)
8. Tzevelekas, L., Stavrakakis, I.: Random Walks with Jumps in Wireless Sensor Networks. Poster session of the 6th IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), Corfu, Greece (June 2007)
9. Penrose, M.D.: Random Geometric Graphs. Oxford Studies in Probability. Oxford University Press, Oxford (2003)
10. Le Boudec, J.-Y., Vojnovic, M.: Perfect Simulation and Stationarity of a Class of Mobility Models. In: Proc. of the 24th IEEE Conference on Computer Communications (INFOCOM), March 2005, vol. 4, pp. 2743–2754 (2005)

Distributed Algorithm for Self Organizing LTE Interference Coordination

Ingo Karla

Bell Labs, Alcatel-Lucent
Lorenzstraße 10, 70435 Stuttgart, Germany
ingo.karla@alcatel-lucent.de

Abstract. A novel generic distributed algorithm is presented, which assigns in a self organizing way resources to the cells in cellular networks under the constraints that resource restrictions need to be considered between the cells. The algorithm operates in a fully distributed way, running independently inside each base station without any central entity. It optimizes the resource assignment, is capable to resolve sub-optimal aspects as well as comprises methods to detect and resolve possible instabilities such as contradicting decisions like ping pongs of two neighbouring base stations. The algorithm is here applied for LTE inter-cell interference coordination and simulations have shown that this distributed algorithm is always capable to solve reliably the resource assignment task.

Keywords: Distributed Algorithm, Colouring, Self Organizing Networks, SON, Self-X, Inter-Cell Interference Coordination, ICIC, IFCO, Cellular Network, 3GPP Long Term Evolution, LTE.

1 Introduction

Self organizing functionalities will play a key role in future wireless networks in order to manage the increasing complexity, to optimize the system performance and to reduce the costs of operation. Self Organizing Network (SON) aspects are being standardized by 3GPP LTE [1], are in demand by network operators driven by the "Next Generation Mobile Networks" alliance [2], and are investigated by European research projects [3][4][5].

The inter-cell interference in cellular networks is handled in 2nd generation mobile networks, like GSM, via the use of different frequencies for neighbouring cells while 3rd generation networks, like UMTS, benefit from spreading code gains of the used WCDMA technology. In contrast, fourth generation mobile networks, such as "Long Term Evolution" (LTE), use an OFDM air interface and are designed to be a frequency "reuse 1" system, i.e. all cells in an operators network use the same frequency band. Thus, the inter-cell interference becomes an important issue and a coordination of resources [6] between cells, i.e. a coordinated use of selected OFDM sub-carriers, increases the system performance, the cell edge throughput and improves the handover robustness [7]. There are several Inter-Cell Interference Coordination (ICIC)

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 119–128, 2010.

approaches including spatial multiplexing and MIMO techniques [8], dynamic methods on a very short scheduler time scale [9], semi-static approaches [10] as well as basically static cell configurations such as Soft/Softer/Partial Frequency Reuse where a cell utilizes in its outer area only a small fraction of the available frequency resources [11][12]. A powerful static ICIC technique is the "inverted fractional frequency reuse" [13][14] which will be outlined below in chapter 2.

All those ICIC mechanisms require resource coordination between cells. Currently, such cell resource assignment tasks, like frequency planning for GSM networks, have usually to be performed manually in a centralized manner by operators with the help of planning tools. For the upcoming LTE systems, those cell resource assignment tasks shall now be carried out automatically, fully distributed in the network.

This self organization task requires suitable algorithms which coordinate and assign the resources among cells. Their interactions and restrictions can be described mathematically via the formulation of the graph theory, based on which self organizing resource allocation can operate [6]. In the context of ICIC, several approaches and algorithms have been investigated with various study foci, with different levels of complexity and on different timescales. Such algorithm studies include fast virtual scheduling algorithms [9], beamforming with interference graphs between mobile terminals [15], centrally controlled dynamic channel allocation [16], decentralized algorithms applied for WLANs [17], distributed algorithms using approaches from game theory [18], as well as distributed two step algorithms [19].

This paper presents and studies a fully distributed self-organizing algorithm for this here presented static ICIC application in LTE, it is especially designed to handle efficiently the computational complexity and to ensure always a stable running radio network even under sub-optimal graph-colouring situations. The paper is structured as follows: Chapter 2 recalls the interference coordination approach at the example of which the generic algorithm is applied. Chapter 3 then outlines the distributed algorithm of which the performance and robustness is shown in chapter 4 by simulations. The paper finishes with a conclusion.

2 Interference Coordination and Self Organization Task

The interference coordination mechanism “inverted fractional frequency reuse” [20][21][13][14] reduces the transmission power for each cell of a fraction of the frequency band i.e. for certain Physical Resource Blocks (PRBs). Mobile terminals in the cell edge area are served with full power by its serving base station on specific PRBs, while the other neighbouring cell has a reduced power level on exactly this part of the frequency band, so that this mobile terminal receives less interference from its neighbouring cell. This is depicted in figure 1, where mobiles served by the red cell and located near the border of the blue cell are scheduled on PRBs of the frequency band 3.

As a result, each cell has to select a particular fraction of the frequency band, on which the relative transmission power is reduced. This selection of a part of the frequency band is also be called in this paper as assigning a colour to this cell.

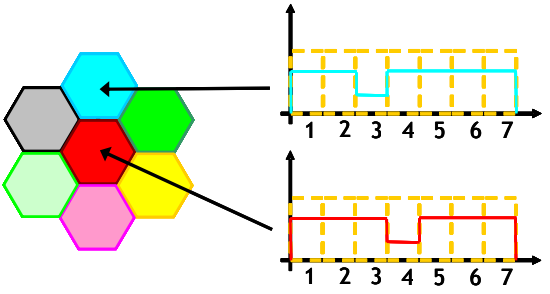


Fig. 1. Illustration of the ICIC with fractional frequency reuse 7/6

Directly neighbouring cells must reduce different parts of the frequency band, in order to be able to apply the described ICIC mechanism between them. In the case that two neighbouring cells should reduce the same one, then there is no interference coordination benefit between these two cells, but the LTE system is still in operational mode, like in the pure cell reuse 1 scheme without any ICIC.

This resource assignment corresponds to a kind of frequency planning. To support the network operators preference for limited operational cost, this planning should not be done manually with a planning tool, but instead the resources are assigned to the cells in an autonomous self organizing way.

3 ICIC SON Algorithm Description

An algorithm is here presented which assigns the resources, labelled by colours, to the cells in a self organizing way; it is a fully distributed algorithm, running in the eNBs for every cell, i.e. without any central entity.

The algorithms aim to assign colours to cells in such a way that two neighbouring cells have different colours, and that same colours are as far separated as possible in order to minimize interferences.

The cell colouring algorithm bases its decisions on the 3GPP specified Neighbour Relation Tables (NRT), from which it is derived between which cells a colour coordination has to take place.

3.1 Distributed Algorithm

Scenario creation/update: At the beginning, each cell collects or receives information about other cells in its surrounding area; in particular the cell stores the known neighbour relation tables (NRT), including the NRT of its neighbouring cells, as well as of all involved cells the already assigned colours – if any. Based on this information, the distributed algorithm calculates how to assign colours in the best possible way.

The algorithm inside each cell comprises two major steps, a fast initial self colouring attempt, followed by later optimizing the situation in the local area around this cell.

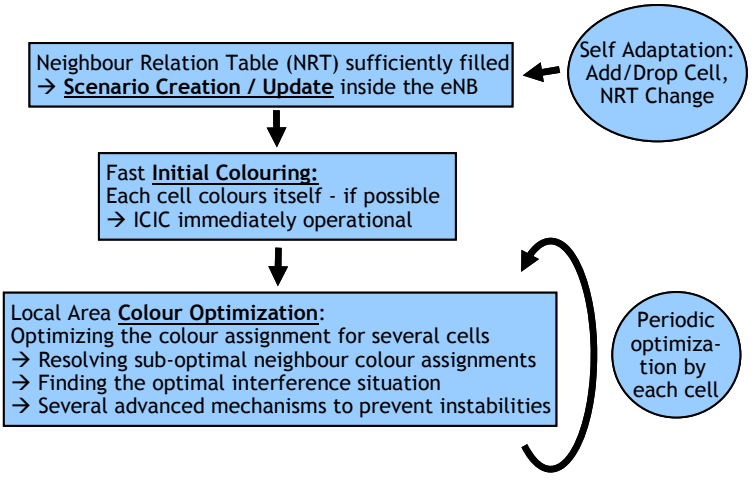


Fig. 2. Simplified flow chart of the distributed resource assignment algorithm

Fast initial self colouring: When a new cell is switched on in the network and after its neighbour relation table (NRT) is sufficiently filled, then the first algorithm step is triggered after a random amount of time. Then, this cell attempts to select a colour for itself, a colour which is not already used in the neighbourhood. If no suitable colour can be found, then for now no colour is taken, and the cell does not yet use ICIC. This initial self colouring algorithm step is very fast, requires very little computation time and ensures that ICIC is quickly operational in many – but usually not in all – cells.

Local area colour optimization: This algorithm step determines the best suited colour assignment for all cells within a local area, for the centre cell and for a set of cells within the neighbourhood. In particular, this local area optimization step has the possibility to assign or change the colour of another cell. If e.g. the colour of a neighbouring cell is changed, then the algorithm can ensure that this colour change does not create a pair of same coloured cells around that neighbouring cell, because also the neighbours of neighbours are known. In such a way, each cell optimizes locally –if necessary– the colouring situation in its surrounding which leads to that the whole network deployment gets coloured with optimal local colour assignments.

Stability/Convergence: It may occur that distributed decision entities come up with contradicting or non-aligned decisions which may lead to Ping-Pong behaviour and non-converging waves of changes. The algorithm comprises functionalities to monitor the situation and to detect possibly occurring Ping-Pongs based on history information. If a Ping-Pong –or a Ring-Ping-Pong involving several cells– should occur, then the optimization procedure determines a particular cell colour arrangement to break this Ping-Pong loop. Furthermore, the algorithm comprises measures to keep the distributed system stable; the optimization procedure determines especially cell-colour arrangement solutions, which restricts the effects of actions to a local area, and thereby prevents that a single change may lead to a moving wave of changes through the network.

Triggers: At the beginning, each cell triggers itself once the fast initial cell colouring algorithm step. Thereafter, the local area colour optimization procedure is triggered periodically and reacts in the case that any cell colours have changed in its surrounding area. Furthermore, the algorithm is also triggered when the neighbour relation situation has changed within the local area. After having updated the local area scenario, the algorithms steps are triggered and the new situation is optimized. In this way, the system monitors itself, adapts to modified situations, like when a cell has been added or removed or when an NRT has been changed. In this way, the system manages to heal itself and to recover from any occurring sub-optimal situations.

3.2 Information Exchange and Signalling

The algorithm bases its decision on certain knowledge of the surrounding cells, on knowing NRTs of other cells and on knowing the already assigned colours of other cells. Concretely, the local algorithm in one cell needs to know at least, which cells are direct neighbours, and the NRT of those neighbouring cells, as well as the colours of all cells involved. Thus, the algorithm knows the colours of all cells within the first and second tier of cells and the NRTs of the cells within only the first tier of neighbouring cells. Then the algorithm has the knowledge to assign colours to neighbouring cells while ensuring that that no neighbour cell has the same colour as one other cell in its surrounding.

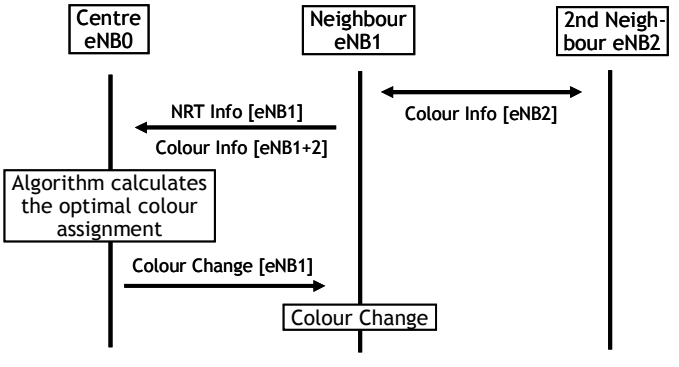


Fig. 3. Signalling message flow chart for the minimal required information exchange between cells

The required signalling is in supported by the LTE Release 8 specification. The NRT is already exchanged between neighbouring base stations via standardized protocol messages over the X2 interface. The colour information and the colour change command or suggestion could be transmitted within a private message, which is also supported by the LTE specification. Figure 3 shows an example for a simple information exchange with the minimal knowledge range. In an equivalent way, it is also possible to obtain information from a larger area of surrounding cells and to perform the optimization including more cells.

4 Algorithm Performance Analysis

This algorithm was validated and its performance was analysed with the help of a LTE system simulator.

4.1 Simulation Environment

The resource assignment algorithm is incorporated into an LTE system simulator based on the IKR Simlib [22]; this LTE simulator determines the NRT of all cells with the help of mobile terminal measurements on the simulation area. The simulator interacts with a graphical display program to illustrate the current colouring of all cells and which allows to add and remove cells.

4.2 Scenario Configuration

Simulations were performed on a variety of different cell arrangements and with a variety of different configuration parameters. The here presented simulations were carried out on a diverse simulation playground with 3781 cells consisting of a mixture of omni-directional, tri-sectorized and six-fold LTE base stations on a hexagonal grid as well as empty areas.

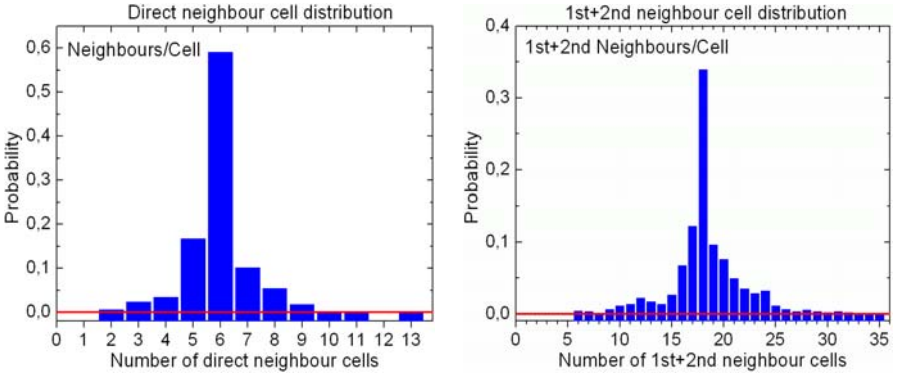


Fig. 4. Distribution of the number of direct neighbours (left) and of first+second order neighbours (right) per cell for the here presented cell arrangement

The complexity of these cell interactions on this simulation playground can be characterized by that on average one cell has 5,9 directly neighbouring cells (maximal 13) and that on average a cell has 18,3 first and second tier neighbours (maximal 35), as illustrated in figure 4.

4.3 Simulations

System simulations of the proposed ICIC scheme had shown [23] that it is the best balance between interference gain and lost capacity due to non used PRBs, to separate the frequency band into 7 different fractions. Thus, the algorithm was evaluated by

default with 7 different colours; other numbers of allowed colours are presented here to show how the algorithm performs in scenarios with different levels of complexity.

Based on that scenario which simulates most realistically a real LTE deployment, typical parameters to obtain the NRT and 7 colours, the distributed algorithms easily solve the colouring problem without that any directly neighbouring cells get assigned the same resources.

The left figure 5 shows the percentage of cell pairs, where two directly neighbouring cells have the same colour; the right figure 5 shows the percentage of cell relations, where one cell has two direct neighbours which have the same colour; this is defined as second order neighbours.

In fact, the distributed algorithm is so powerful, that already 5 different colours are sufficient to solve the resource assignment task without that two neighbouring cells have the same colour. With only 4 different colours, about 0.45 % of the direct neighbour relations suffer that two neighbouring cells have the same colour, which prevents ICIC to operate between these two cells. Figure 6 shows as an example the successful colouring of a small playground with 305 colours with 7 different colours.

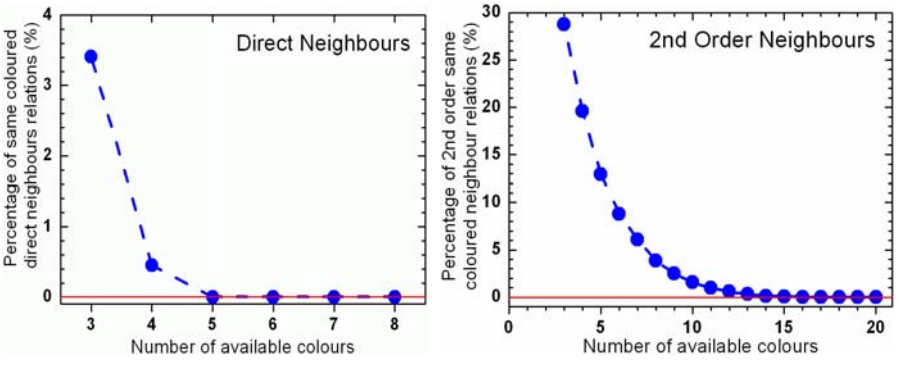


Fig. 5. Performance of the algorithm with different amounts of available colours.
Left: Percentage of the direct neighbour relations, where two directly neighbouring cells have the same colour.
Right: Percentage of the first and second order neighbour relations, where first or second order neighbour cells have the same colour.

For the ICIC, it is of advantage to have same resources separated as far as possible in order to minimize possibly occurring interferences. In order to achieve this, the centre cell needs to have a different colour than all cells in the first and second tier of neighbours, i.e. a coordination with on average 18,25 cells, and there exist no perfect first+second order colour arrangement with only some available colours. For example with the typical configuration of 7 different colours, around 6% of second order neighbours relations are between second order cells with the same colour.

In most cells, the algorithm converges very fast, if an optimization is necessary after the initial colouring situation, then in most cases one or maybe two optimization procedures are sufficient to reach the final colour assignment. It may in distributed

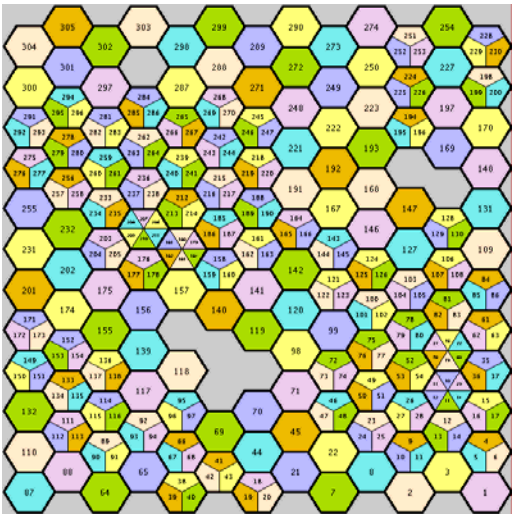


Fig. 6. Example of a small simulation area with 305 cells and with 7 different colours. The distributed algorithms manage to assign the resources in such a way that no neighbouring cells have the same colour.

decision entities occur, that different cells take contradicting decisions, such ping-pong effects are sometimes observed in the simulations. The algorithm mechanisms detected these ping-pongs, and with subsequent optimizations these ping-pongs are resolved safely, so that a good and stable resource distribution was always reached.

In addition to being able to colour a new, empty playground, the algorithm is also able to react on changes in the scenario. In the simulator, this can be emulated by adding or removing cells, then via mobile terminals the new radio conditions and new/modified NRTs are created in the cells. In all cases, the algorithms detected these changes and always managed to adapt –if necessary– the cell resource assignments and to achieve an optimal re-organization of the resources in this new situation.

The algorithm was implemented in a SON ICIC demonstrator for LTE and the self organizing algorithm functionality and performance has recently been demonstrated publicly on large exhibitions [24][25]. There, the algorithm operation has also been visualized in real time, how the distributed algorithms manage to assign and re-arrange the cell resources and how they immediately adapt to changed cell layout situations.

5 Conclusion

This distributed algorithm always manages to assign reliably the resources to the cells in a self organizing way. In all investigated situations, this algorithm was able to achieve in the best possible way its resource assignment aims and the algorithm is self adapting to changed situations. This algorithm has been designed for and is here demonstrated at the example of ICIC in LTE Release 8, but it is a generic algorithm which

is also applicable for other self organizing tasks, where any resources need to be coordinated and assigned to e.g. cells with certain restrictions.

This ICIC mechanism and its self organizing algorithm are transferred from Bell Labs to be implemented in Alcatel-Lucents LTE product. Furthermore, this self organizing algorithm is the basis for our ongoing product development of self organizing semi-static ICIC, which operates on a shorter time scale and considers the current load situation in the cells.

Acknowledgements

I thank Hajo Bakker, Lutz Ewe and Oliver Blume for fruitful discussions and for their support.

References

1. 3GPP TR 36.902, Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Self-configuring and self-optimizing network (SON) use cases and solutions, http://www.3gpp.org/ftp/Specs/html-info/36902.htm
2. Next Generation Mobile Networks (NGMN) Alliance: NGMN Recommendation on SON and O&M Requirements, http://www.ngmn.org/nc/downloads/techdownloads.html
3. SOCRATES, Self-Optimisation & self-ConfiguRATion in wirelEss networkS, http://www.fp7-socrates.eu/
4. End to End Efficiency, E^3, https://ict-e3.eu
5. Belschner, J., Arnold, P., Eckhard, H., Kühn, E.: Optimisation of Radio Access Network Operation introducing Self-x Functions. In: Vehicular Technology Conference, Barcelona, Spain, April 26-29 (Spring 2009)
6. Aardal, K.I., van Hoesel, S.P.M., Koster, A.M.C.A., Mannino, C., Sassano, A.: Models and solution techniques for frequency assignment problems. Annals of Operations Research 153(1), 79–129 (2007)
7. Aziz, D., Sigle, R.: Improvement of LTE Handover Performance through Interference Coordination. In: Vehicular Technology Conference, Barcelona, Spain (Spring 2009)
8. Andrews, J.G., Choi, W., Heath Jr., R.W.: Overcoming Interference in Spatial Multiplexing MIMO Cellular Networks. Wireless Communications 14(6), 95–104 (2007)
9. Stolyar, A.L., Viswanathan, H.: Self-organizing Dynamic Fractional Frequency Reuse for Best-Effort Traffic through Distributed Inter-Cell Coordination. In: INFOCOM 2009, Rio de Janeiro, Brazil, April 19-25, pp. 1287–1295 (2009)
10. R1-07-3187, Interference Coordination Framework with Results; 3GPP TSG RAN WG1 #49bis Meeting, Orlando, USA, June 25-29 (2007)
11. Xiang, Y., Luo, J., Hartmann, C.: Inter-Cell Interference Mitigation through Flexible Resource Reuse in OFDMA based Communication Networks. In: European Wireless 2007, Paris, France, April 1-4 (2007)
12. Zhang, X., He, C., Jiang, L., Xu, J.: Inter-Cell Interference Coordination Based On Softer Frequency Reuse in OFDMA Cellular Systems. In: Conference Neural Networks & Signal Processing, Zhenjiang, China, June 8-10 (2008)
13. R1-06-1455, System-Level Simulations for Evaluation using Downlink Interference Coordination; 3GPP TSG RAN WG1 #45 Meeting, Shanghai, China, May 8-12 (2006)

14. R1-06-2365, Comparison of efficiency of DL Interference Coordination schemes and view on measurements on intra frequency neighbour cells; 3GPP TSG RAN WG1 #46 Meeting, Tallinn, Estonia, August 28-September 1 (2006)
15. Necker, M.C.: Local Interference Coordination in Cellular OFDMA Networks. In: Vehicular Technology Conference, Baltimore, USA, September 30 - October 3, pp. 1741–1746 (Fall 2007)
16. Tan, H.C., Gurcan, M.K.: A fast dynamic channel allocation scheme for a centrally controlled radio local area network. In: Vehicular Technology Conference, Atlanta, USA, April 28- May 1, vol. 2, pp. 731–735 (1996)
17. Leith, D.J., Clifford, P.: Channel Dependent Interference and Decentralized Colouring; Network Control and Optimization, pp. 95–104. Springer, Heidelberg (2007)
18. Ellenbeck, J., Hartmann, C., Berlemann, L.: Decentralized Inter-Cell Interference Coordination by Autonomous Spectral Reuse Decisions. In: European Wireless Conference 2008, Prague, Czech Republic, June 22-25 (2008)
19. Chang, Y.J., Tao, Z., Zhang, J., Kuo, C.C.J.: A Graph based Approach to Multi-Cell OFDMA Downlink Resource Allocation. In: Global Telecommunications Conference 2008, New Orleans, USA, November 30- December 4 (2008)
20. R1-050272, OFDM air interface with QoS at cell edge; 3GPP TSG RAN WG1 #40bis Meeting, Beijing, China, April 4-8 (2005)
21. R1-050594, Multi-cell Simulation Results for Interference Co-ordination in nes OFDM DL; 3GPP TSG RAN WG1 LTE Ad Hoc on LTE, Sophia Antipolis, France, June 20-21 (2005)
22. Simulation Library, I.K.R.: University of Stuttgart, `http://www.ikr.uni-stuttgart.de/INDSimLib/`
23. Alcatel-Lucent internal study: Downlink LTE simulations
24. Alcatel-Lucent SON ICIC Demonstration, World Mobile Congress 2009, Barcelona, Spain, February 16-19 (2009)
25. Alcatel-Lucent SON ICIC Demonstration, CeBIT 2009, Hannover, Germany, March 3-8, (2009)

Session 5:
Algorithms and Applications

Design and Implementation of a Radio Access Selection Algorithm for Multi-mode Mobile Terminals

Alexandros Kaloxylos[1], Fotos Georgiadis[2], Ioannis Modeas[2], and Nikos Passas[2]

[1] Department of Telecommunications Science and Technology
University of Peloponnese, Tripoli, Greece
[2] Department of Informatics and Telecommunications,
University of Athens, Athens, Greece
kaloxyl@uop.gr, {fotos,imodeas,passas}@di.uoa.gr

Abstract. Modern mobile terminals giving access to multiple radio access technologies at the same time allow users to select specific technologies and/or different operators for their services. This calls for an automated radio access selection mechanism. In this paper we propose such a mechanism with several novelties: i) it enables terminals to build prioritized lists of target access networks independently for each of their active connections; ii) it aims to satisfy user preferences instead of providing a mere load balancing between networks; iii) it is designed to operate with two decision-making points (mobile terminal and core network), splitting the complexity of the overall process. We discuss the main functionality of the proposed mechanism, its prototype design in SDL and specific details of our test-bed implementation using open source tools.

Keywords: 4G, radio access selection, multi-mode terminals.

1 Introduction

During the past years we are witnessing an increase of mobile phones that are equipped with more than one network interfaces and capabilities that characterize a small PC. The mobile operators deploy additional radio access technologies (e.g., WiFi, WiMAX), so that they can increase network utilization and provide for better services to the users. The idea is to use load-balancing mechanisms that will enable traffic sharing between different Radio Access Technologies (RATs). Thus, we end up with a heterogeneous environment, where users are flexible enough to select the most suitable RAT for their needs, while operators wish to enforce their policy and maximize utilization of their resources. In such heterogeneous environments, automatic RAT selection plays a crucial role in the functionality of the whole network. Most of the existing proposals focus on the selection of the "most suitable" target RAT during a handover (HO) execution or the establishment of a new call. Cost functions [1], fuzzy logic [2], neural networks [3] and policy-based schemes [4-6] are the candidates to tackle the issue.

Almost all of these algorithms have been designed with a single decision point, where all contextual information is evaluated. Their goal is to have either the user or

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 131–142, 2010.

the operator to decide about the best RAT. Obviously, the interests and preferences of these two players are not always the same. Thus, the proposals either imply a future scenario where users will have total control over selecting operators and RATs, or a case that is closer to the current status where the operator has total control. Moreover, most of these proposals consider all a user's connections to be handled by the same RAT. This is a rather monolithic approach and by no means needs to be like this in the future. The terminals will be able to have active connections through different interfaces. For those proposals that suggest such a flexible management of connections, no implementation details are provided. Finally, most of the proposed mechanisms focus on the decision mechanism and do not provide information about how the additional functionality can be integrated into existing standards.

Having these issues in mind, we have designed and implemented a new RAT selection mechanism, where each connection of a Mobile Terminal (MT) is handled separately. This provides more flexibility on fine-tuning the available resources and at the same time increasing the user's satisfaction [7]. It is also split in two cooperative parts, at the MT and the network side. The MT part builds a prioritized list of associations between available RATs and active connections. The network part attempts to satisfy the top priorities of the user as long as there are adequate resources and the speed and direction of a user make the selection of a RAT meaningful (e.g., a WiFi should not serve a rapid moving user). This split of functionality allows alleviating the core network from certain processing load since some pre-processing is performed at the MT side. Moreover, several cases that can be evaluated and stopped in the MT will do so resulting in a significant reduction of unnecessary signaling exchanges. We expect that this does not place a serious burden in modern MTs that already have appreciable and all increasing processing power, memory storage capacity and battery longevity.

In the implementation of our mechanism we used Mobile IP (MIP), which is expected to be the de facto standard for mobility management. The mechanism can be used as-is in a loosed-coupled architecture but it can also be used in tight-coupled schemes as long as the appropriate extensions are provided to existing UMTS protocols [7]. The mechanism does not require complex calculations since initial processing is executed in the MT, while the final decision is taken inside the core network, allowing both sides (the user and the operator) to enforce their policies. The final decision is a trade-off between the user preferences, the terminal capabilities, the network load and the location and speed of the MT.

The remainder of the paper is organized as follows. Section 2 presents both parts of the proposed algorithm in detail. In section 3 we provide information about a prototype we have build using the Specification and Description Language SDL [8] and implementation details of our test-bed. Finally, section 5 concludes the paper.

2 Description of the Proposed Algorithm

The proposed distributed algorithm is split in two distinct and cooperating parts, the first running in the MT and the second in the core network. Its main output is the decision of the most suitable RAT during a new call establishment or upon a HO execution. The latter may be a horizontal (intra-RAT) HO, in which case the access

technology supporting a connection does not change, or a vertical (inter-RAT) HO, in which the supporting technology changes. The RAT selection is performed as a trade-off between the user preferences, the MT location and speed and the load of each RAT involved. The user preferences indicate which of the available RATs is preferable for each service provided. Although the algorithm has been designed to operate in environments where multiple heterogeneous radio access technologies exist, the subsequent section describes a case study with two access networks, namely UMTS and WLAN.

2.1 Algorithm Running in the Mobile Terminal (MT)

The MT part takes under consideration parameters located in the user profile and specifically the user's preferences related to the cost, the QoS and the battery duration. Also, the service requirements related to the Received Signal Strength (RSS) (error rates, delay, etc.) and the MT characteristics related to the power consumption of its radio interfaces. This algorithm is presented in Fig. 1. Its main purpose is to build prioritized lists of target RATs that are compatible with the user preferences. This is performed independently for each connection, either active or new, in order to provide for more flexibility and better user satisfaction. Five different stimuli may invoke the execution of the algorithm (cases (i)-(v) in Fig.1).

i) The MT has at least one active connection and a new RAT with strong enough radio signal is detected. This detection is based on the RAT dependent functionality of a new access point discovery. Next, the MT creates a two-dimensional priority list of N rows and M columns, where N is the number of active connections and M the number of alternative RATs. This priority list is filled in accordance with the user profile. As a next stage, the algorithm checks if all RATs involved in the previous step provide adequate radio link quality to support the requested services (e.g. through the radio signal strength – RSS – indicator). If a RAT does not fulfill these requirements, it is eliminated from the list. Next, the MT calculates the battery consumption for the simultaneous operation of all interfaces involved and modifies the priority list according to the importance the user gives to the battery duration. At this point, the list is sorted in descending order per line (i.e., connection) so that each line finally contains the alternative RATs for one particular connection, starting from the one that serves it best to the one that serves it worst. This list is sent to the core network along with a message requesting a HO.

ii) A forced HO command is received from the core network, concerning specific or all connections of the MT. This may be due to load balance purposes and is decided by the operator's network components. Thus, the time restrictions are not very tight, since the network operator should not initiate such a HO at the very last moment. Since the time restrictions are not very tight, this case is treated the same way as the previous one. As in the previous case, an effort is made to consider the user preferences, under more restrictive patterns this time, since some RATs may not be permitted if they are overloaded.

iii) A new call is initiated. The MT may be idle or have active connections. This time the algorithm considers the user preferences from the user profile and the battery condition and creates a list of prioritized RATs only for the new connection. Then it sends to the core network a message indicating the new call initiation along with this

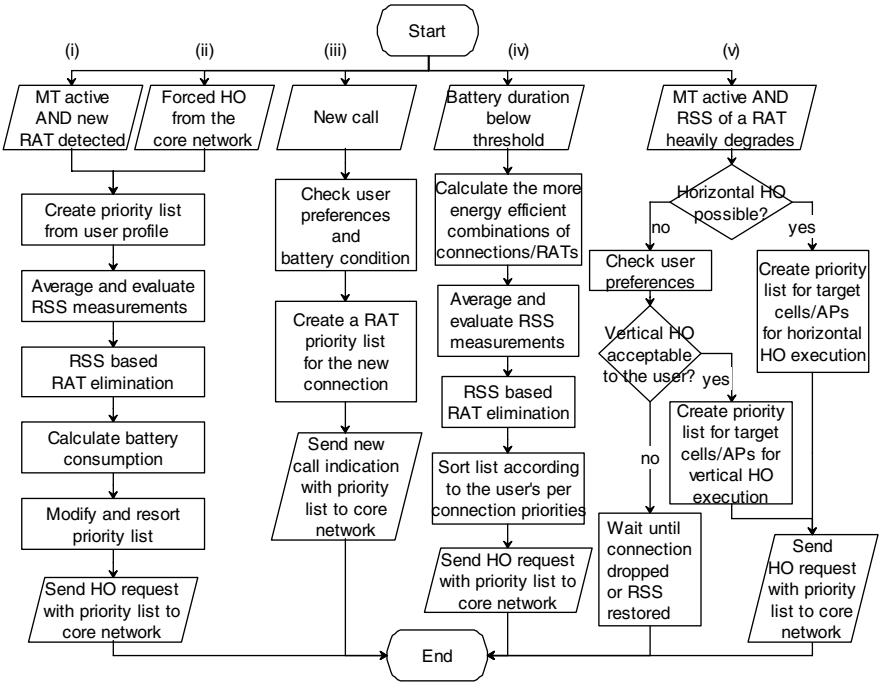


Fig. 1. Algorithm in the Mobile Terminal (MT)

priority list. The algorithm does not re-evaluate all active connections since this may only be necessary in case of low battery life. This case is taken care of from the next trigger.

iv) The remaining battery duration falls below a certain threshold, whose value is a user dependent factor and may be incorporated in the user profile. In this case, the MT finds which combinations of connections and RATs are the more energy efficient. This is feasible, since the MT is aware of the power consumption of each interface. Then, it eliminates all RATs with inadequate signal quality for each connection, so it rejects some of the combinations it just calculated. The remaining combinations are sorted according to the priority the user gives to each particular connection. This will allow the core network to reject, if required, the least important connections in case that the combinations sent cannot all be fulfilled.

v) The MT is active and the collected RSS measurements indicate a degrading signal from a RAT and an imminent HO. So, if a horizontal HO is feasible, a HO request is send to the core network along with a list of candidate cells/APs. The possibility of a vertical HO is considered only if a horizontal HO is not possible, i.e. there are no access points of this particular RAT in vicinity. Such a case could be when a WLAN connection has to be handed over, because the MT is moving out of the coverage area and there are no neighboring APs to be served by, and keep the connection within the WLAN. So, if it is acceptable, a similar procedure as before is followed. If not, there is no action and either the connection will be dropped as a result of radio

link degradation, or the signal may be restored (e.g. change of user direction movement) and the connection goes on.

2.2 Algorithm Running in the Core Network

The part of the algorithm running in the core network takes the final decision about the admittance of a new connection or the HO of an existing one ((i)-(iii) in Fig. 2). All these triggers are the messages received as the result of the corresponding algorithm at the MT, described in the previous subsection.

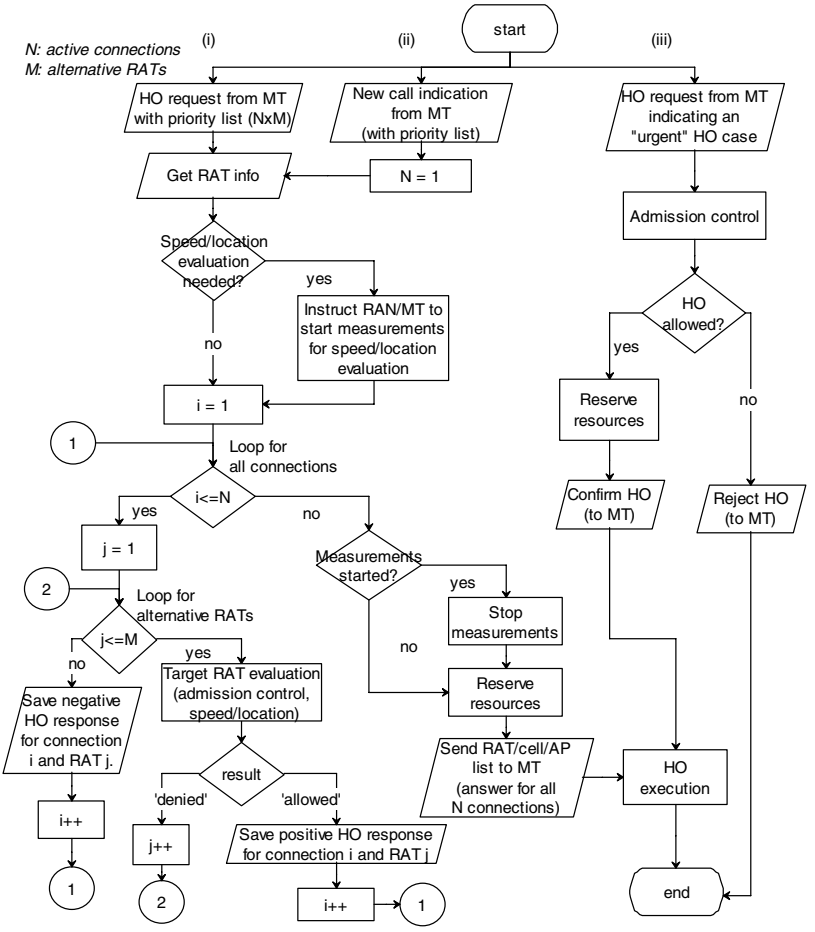


Fig. 2. Algorithm in the Core Network.

i) The first trigger is a HO request message sent by a MT to indicate the need to re-evaluate all its active connections. The priority list as formed by the MT algorithm is received as well. If the selection of a specific RAT implicates location and speed considerations, e.g. a limited range WLAN, then the procedure for their evaluation is

started. This is required since it is meaningless to HO to an AP if the MT's speed is very high and will leave the AP's coverage in few seconds, or if the MT is near the AP's border coverage and moving away from it [9].

At the next step a nested loop is started. The outer loop corresponds to the number of active connections. The inner loop is for the M alternative RATs of each connection. Thus, for each connection i (i = 1, …, N) every alternative target RAT is evaluated, starting from the first one, since this was the decision taken by the MT after considering the user's preferences. This evaluation for the UMTS case means that the admission control algorithm is executed and the HO to this particular RAT is either 'allowed' or 'denied'. For the WLAN, apart from checking the load of the target AP, the speed and the location of the MT are estimated. When all connections are completed, the core network instructs the termination of the measurements for location and speed tracking. Then an answer to the HO request of the MT is sent back, along with the list of the final RAT choice for each connection.

ii) The second trigger is a new call indication from a MT. This is treated as the previous trigger, where all the connections are evaluated. The only difference, in this case, is that only the connection to be initiated is evaluated, therefore N=1.

iii) The last trigger is a HO request indicating an "urgent" HO. In this case, the admission control algorithm of the RAT selected by the algorithm in the MT is executed and decides upon the HO feasibility. We remind here that the MT has already checked the alternative RATs, and proposes only one of them according to coverage and user preferences. Then, if the HO is allowed, then the HO execution proceeds, else the MT is informed about the HO rejection.

3 SDL Prototype and Test-Bed Implementation

In Fig. 3 we present the top level of our SDL system. The purpose of using SDL prior to the implementation is to have a rapid prototype and check the validity of our design. The SDL system has been implemented in SDL using Telelogic's SDL-Suite tool [10]. After the specification completion the model was validated using SDT simulation tools, for different scenarios. The MT is connected to a UMTS and a WLAN for the exchange of data information. It is also connected directly with the module NDP (Network Decision Point) that is the network part of our mechanism. In this figure, the reader can also note that we use a block to model the Home Agent (HA) for the terminal, as well as a Correspondent Node (CN). The main target of this system is to demonstrate a functionality where the MT is communicating with the CN through UMTS or WLAN based on certain contextual information. This information (e.g., signal strength, speed and direction of the MT, level of congestion inside a network, level of battery in the MT) is provided during the guided simulation. What we have checked with this validation model is that our mechanism works smoothly during the establishment of a new connection or the execution of a vertical handover between networks in every test case scenario.

One main assumption we have made during the design and implementation of our mechanism is that the MT will always have access to the UMTS network. This is because a UMTS network is expected to be ubiquitous while other RAT technologies such as WLAN are expected to have discontinuous coverage areas. Thus, any

signaling exchange between the MT and the NDP is done through the UMTS network. Thus, in Fig. 3 there is only a channel between NDP and UMTS, but not between NDP and WLAN. Also, the MT is communicating directly with the NDP block for reasons of simplicity. During SDL simulation the MT link with the UMTS (and in this case with WLAN) is used just for the exchange of data between the MT and the CN. In our architecture, we have assumed the use of a loose coupling scheme between the UMTS and the WLAN networks. This means that the NDP entity can be placed on top of the GGSN (gateway GPRS support node) network component of UMTS. Although this implies a higher delay for the exchange of signaling between the MT Decision Point (MTDP) and NDP entities, it requires no modification at all on existing standards.

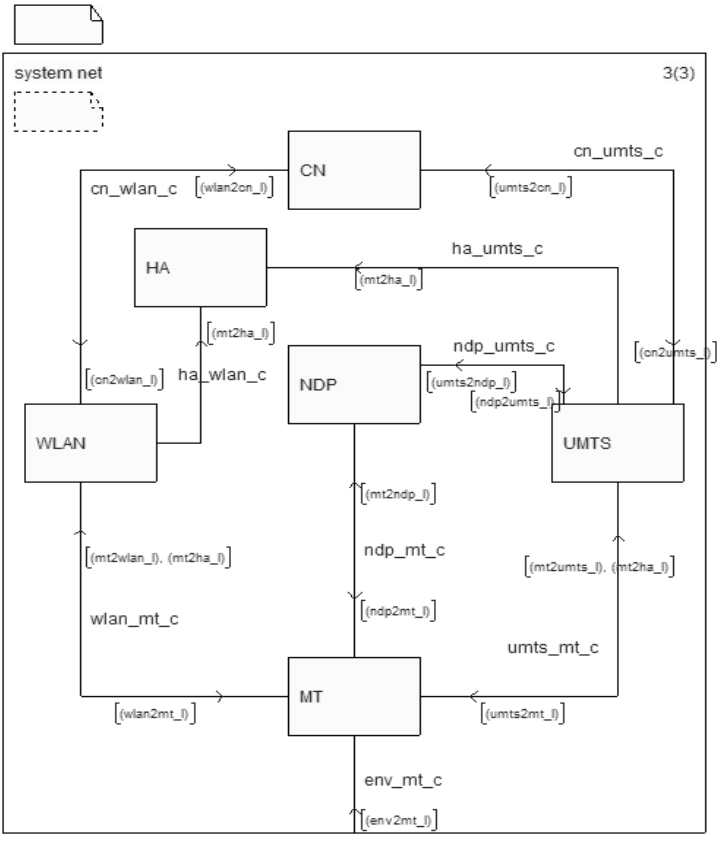


Fig. 3. Logical Architecture in SDL

Moreover, note that the HA has links with both the UMTS and the WLAN, since after the MT selects an interface for its connection and finalizes the association with the respective network it requires the appropriate message exchange for receiving a new IP address and to notify the HA about this.

Next, we discuss the implementation details of our mechanism in an appropriately configured test-bed and present the scenarios we have tested. More specifically, and due to the lack of real UMTS equipment, we have deployed two IEEE 802.11 Access Points (APs). One of them plays the role of the UMTS network, transferring all the signaling between the MT and the core network. Our mechanism comprises the two entities, one located in the terminal and the other in the network. The two entities exchange messages in order to decide the access network through which an active or new connection will be served. These entities take into consideration several pieces of information, such as the monetary cost, the network load, the signal strength, the battery level etc. Some of these characteristics are collected from the operating system of the devices or are hard-coded due to lack of appropriate equipment.

The whole test-bed is based on Linux. The distribution used in the APs is OpenWrt [11], a Linux distribution appropriately configured for use in embedded devices, enhanced with IPv6 functionality. This distribution was chosen because it supports the necessary flexibility for routing and an easy way to reach network statistics through the SNMP protocol. The Network Mobility / NEMO Platform for Linux (NEMO/NEPL) implementation [12] is used for mobility support, since at the time of the deployment of our test-bed it was the most stable open source implementation. The NEMO protocol is an extension of Mobile IP that supports mobility of entire networks. Network mobility arises when entire networks are changing their point of attachment with respect to the Internet topology. A mobile network is connected to the Internet via one or more mobile routers (MR). Nodes behind the MR are referred to as mobile network nodes. Thus, NEMO supports moving nodes inside moving networks (e.g., mobile users inside a train). NEMO/NEPL is based on the Mobile IPv6 for Linux (MIPL) stack that has been developed by the University of Helsinki [13]. Currently, the Universal Playground for IPv6 (USAGI project – [14]) task group provides support for MIPL.

In this implementation we have added the required functionality to support Multiple Care of Addresses (CoA) [15]. Multiple CoAs are required since the mobile terminal may have more than one open network interface and thus, requires more than one IP address in order to be reachable on every interface. The standard Mobile IP allows the registration of a single primary care of address with a HA. To have the assignment of multiple CoAs feasible there is a need for an additional identifier called Binding IDentification number (BID). For the needs of the test-bed we used a large IPv6 address space (/40) divided into several subnets. Appropriate routing rules have been setup between the nodes. The overall topology is depicted in Fig. 4. Two WiFi APs act as the different RATs. The direct Ethernet link with one of the APs acts as the ubiquitous UMTS connection transferring all messages between the MTDP and the NDP. The two APs are connected, through an access router, to the Internet and a corresponding node. In this router, the HA and the NDP are located. Moreover, the software for the NEMO mobile router was collocated with the mobile terminal since in our test-bed there was no need to demonstrate moving networks. In the mobile terminal we have also placed the MTDP entity.

As far as routing is concerned we have used the Quagga routing suite [16]. More specifically, we used the OSPF (Open Shortest Path First) protocol that supports routing in IPv6 networks [17]. The choice for dynamic routing, instead of a more static solution, enables the test-bed to be reconfigured easily with additional access technologies and networks.

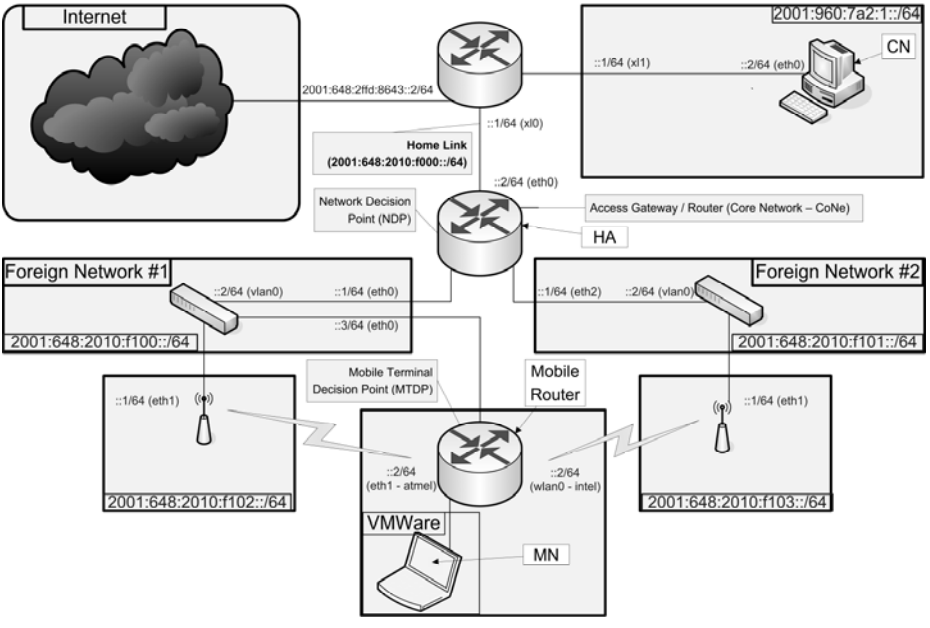


Fig. 4. Test-bed topology

For the automatic IPv6 addressing of mobile nodes, as they are connected to the APs, the Linux IPv6 Router Advertisement Daemon (radvd) was used [18]. The Router Advertisement Daemon advertises mobility options for the Home Link, such as HA availability, preference value and lifetime as well as Mobile Router support capabilities, at the NDP network and the wireless prefixes at the AP attachment points. Its operation is described in [19] and we have used the Linux implementation as described in [18].

Using the aforementioned software, we had to extend the basic NEMO functionality by:

1. defining new headers and messages for the exchange of information between the new entities (MTDP and NDP),
2. extending NEMO with support for multiple CoAs (note that NEMO is still under development and even now the MCoA feature is not fully supported),
3. defining a syntax and grammar used by the policy rules for selecting a RAT,
4. implementing both the MTDP and the NDP.

For the exchange of messages between MTDP and NDP there was a need to build a direct interface between them, however in practice this proved to be difficult. The reason was that before submitting policy messages, between the MTDP and the NDP, the network link must have been established. Delaying this necessary step, while trying to take a decision for a specific RAT and the added the difficulty in controlling the whole NEMO stack with the Multiple CoAs extensions resulted in delays for the execution of handovers. The next best choice was to use existing messages and interfaces to piggyback the required information for our mechanism to work. This way

there is a guarantee that the required information will be exchanged safely between the MTDP and the NDP. Thus, the information needed by the new messages is being transferred as extensions to existing mobility messages (e.g., as Mobility Options in Binding Update and Acknowledgment messages exchanged between the HA and the MT).

The message used for this task is the binding update message that was exchanged every time there was a change on the operating conditions of the mobile terminal as for example when:

i) discovering a new access network,
ii) the signal strength of the current AP is very low,
iii) battery level dropped under a certain threshold.

In the mobile terminal the user preferences are stored in a file together with additional information required for mobility management. The policies for each application can be in the form of a list. For example (WLAN, UMTS) means that for a specific application the first choice is to route the data through a WLAN and if this is not possible (e.g., no WLAN is available in the area, or the WLAN is congested) use a UMTS network as an alternative. In order to simplify this issue for the less experienced users, we can define generic pre-defined lists that will be easily understood by the users.

The test-bed was used successfully in a number of scenarios, which demonstrated that not only the key characteristics of our mechanism actually work, but also that it is feasible to treat each mobile terminal connection separately from the others. This of course is a very important characteristic that enables users to be quite flexible when selecting services from one or many RATs and/or operators. The program we used for recording messages and data traffic was tcpdump that is a well-known and established program [20]. Since tcpdump can be executed in the Linux platform we were able to collect information from several points of the network and even from the APs.

The analysis of the messages was performed using the graphical environment of Wireshark [21]. Using this program we were able to analyze the record files produced by tcpdump and monitor the exact times the messages were exchanged between the entities as well as their payloads. For example, in Fig. 5 we present the data collected by Wireshark when performing a handover while having a ping command active. As shown in the figure, we can monitor all the fields in all layers (e.g., see IPv6 addresses, port numbers), as well as the time these messages were exchanged.

Although in our cases we used real traffic through the Internet, the disruption time during a handover was minimal (in the order of magnitude of msecs). This was also the case when using video streams. The reason for this was that the HA in the testbed is located close to the MT and there were not many terminals requesting responses from the NDP. In a real situation it is expected that the system would present typical disruption times of Mobile IP.

Finally, our implementation has integrated the RAT selection mechanism with an authentication procedure. The authentication procedure includes the exchange of keys with the APs using the EAP-TTLS protocol [22]. These keys are transferred

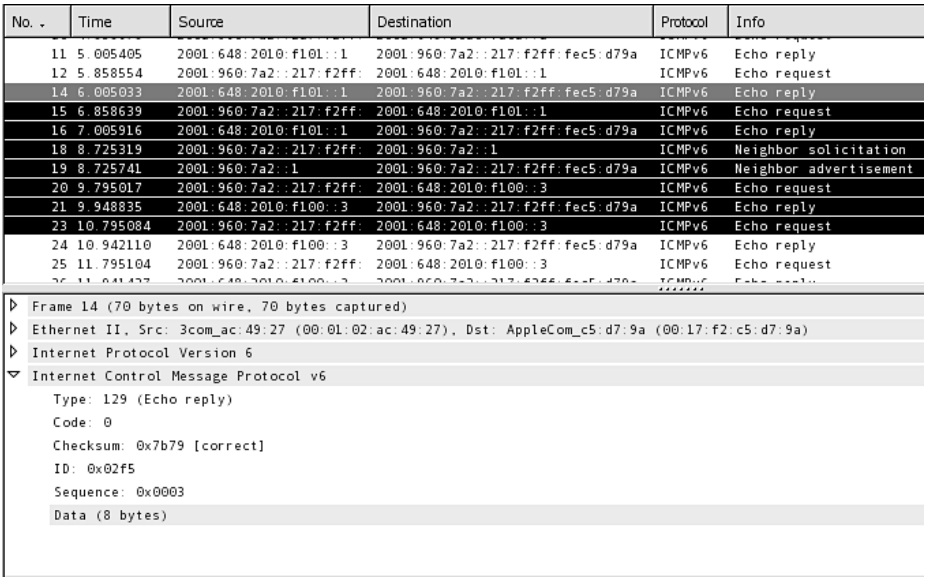


Fig. 5. Example of an ICMPv6 handover

encrypted to a RADIUS [23] server located in the access router. Using this information it will accept or reject the request for a connection.

4 Conclusions

In this paper we have presented a new mechanism for selecting RATs when moving in a heterogeneous environment. The mechanism takes into consideration a number of parameters such as user preferences, signal strength, battery level, network congestion, speed and direction of a terminal, etc. Its main goal is to satisfy the preferences of the users and not merely to load balance the traffic between the available networks. To achieve this, the mechanism has two decision points. The first one is on the mobile terminal and builds a prioritized list of RATs for each one of its connections, based on user preferences. The second decision point is located on the network and checks mainly if there are resources to satisfy user's requests.

The paper also describes an SDL prototype we have built to test the correctness of our mechanism, as well as the implementation of a test-bed that was based on open source software. This test-bed proved the feasibility of our proposal and additionally demonstrated a differentiated treatment of active connections (i.e., having some connections through one RAT while others can be served by a different RAT). It also proved that the ability to execute vertical handovers between RATs is a viable and easy to implement approach. We believe that such a capability will be the standard choice in future networks.

References

1. McNair, J., Zhu, F.: Vertical Handoffs in Fourth-Generation Multi-network Environments. IEEE Wireless Communications 11, 8–15 (2004)
2. Hou, J., O'Brien, D.C.: Vertical Handover-Decision-Making Algorithm using Fuzzy Logic for the Integrated Radio-and-OW System. IEEE Transactions on Wireless Communications 5(1), 176–185 (2006)
3. Giupponi, L., Augusti, R., Pérez-Romero, J., Sallent, O.: A novel Joint Radio Resource Management Approach with Reinforcement Learning Mechanisms. In: 24th IEEE International Performance Computing & Communications Conference, IPCCC 2005, pp. 621–626 (2005)
4. Murray, K., Mathur, R., Pesch, D.: Intelligent Access and Mobility Management in Heterogeneous Wireless Networks using Policy. In: The 1st International Workshop in Information and Communication Technology, pp. 181–186 (2003)
5. Zhuang, W., Gan, Y.-S., Loh, K.-J., Chua, K.-C.: Policy-based QoS Management Architecture in an Integrated UMTS and WLAN Environment. IEEE Communications Magazine 41(11), 118–125 (2003)
6. Song, W., Zhuang, W., Cheng, Y.: Load Balancing for Cellular/WLAN Integrated Networks. IEEE Network 21(1), 27–33 (2007)
7. Lampropoulos, G., Passas, N., Kaloxylos, A., Merakos, L.: A Flexible UMTS/WLAN Architecture for Improved Network Performance. Springer Wireless Personal Communications Journal, special issue on Seamless Handover in Next Generation Wireless Mobile Networks 43(3), 889–906 (2007)
8. ITU-T. International Telecommunication Union, Specification and description language (SDL), Recommendation Z.100, ITU-T Study Group 17 (2009), http://www.itu.int/ITU-T/studygroups/com17/languages/Z100.pdf
9. 3GPP TS 25.305, Stage 2 functional specification of User Equipment (UE) positioning in UTRAN, Release 7 (2006)
10. Telelogic SDL Suite, http://www.telelogic.com/products/sdl/index.cfm
11. OpenWRT Linux distribution for embedded devices, http://openwrt.org
12. NEPL (NEMO Platform for Linux), http://www.nautilus6.org/doc/nepl-howto
13. MIPL – Mobile IPv6 for Linux, http://www.mobile-ipv6.org
14. USAGI Project - Linux IPv6 Development Project, http://www.linux-ipv6.org
15. Wakikawa, R., Ernst, T., Nagami, K., Devarapalli, V.: Multiple Care-of Address Registration, IETF Internet Draft Version 06 (August 2008), http://www.ietf.org/internet-drafts/draft-ietf-monami6-multiplecoa-06.txt
16. Quagga Routing Software Suite, GPL licensed IPv4/IPv6 routing software, http://www.quagga.net
17. Coltun, R., Ferguson, D., Moy, J.: OSPF for IPv6, IETF RFC 2740 (December 1999)
18. Linux IPv6 Router Advertisement Daemon (radvd), http://www.litech.org/radvd
19. Narten, T., Nordmark, E., Simpson, W.: Neighbour Discovery for IP Version 6 (IPv6), IETF RFC 2461 (December 1998)
20. tcpdump / libpcap, http://www.tcpdump.org
21. Wireshark network protocol analyzer, http://www.wireshark.org
22. Funk, P. and Blake-Wilson, S.: Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), RFC 5281 (2008), http://tools.ietf.org/html/rfc5281 (accessed 16/2/2009)
23. Rigney, C., Willens, S., Rubens, A., Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC 2865 (2000), http://www.ietf.org/rfc/rfc2865.txt

Managing of Large Data Artifacts on Mobile Devices with an Ultra Sensitive GPS Devices

Zdenek Slanina and Ondrej Krejcar

VSB Technical University of Ostrava, Center for Applied Cybernetics, Department of measurement and control, 17. Listopadu 15, 70833 Ostrava Poruba, Czech Republic
Zdenek.Slanina@vsb.cz, Ondrej.Krejcar@remoteworld.net

Abstract. Nowadays there is decreasing number of limitations during using commercial mobile devices for data transfer, wireless connectivity or mobile device tracking. The last item is main area of this work. The model of a radio-frequency based system enhancement for user's location and tracking is developed for mobile information systems. The experimental framework prototype uses a few wireless technologies to determine indoor and outdoor position as wireless network infrastructure, global position system (GPS) etc. User location is mainly used for data prebuffering and preload by information system server to PDA or mobile device. All data on the server are saved with its artifacts as the position in the building or outdoor area and used location technology respectively. The reason for prebuffering is high speed of application response when a large amount of data is needed to transfer by server to mobile client.

Keywords: Mobile Device; Localization; Prebuffering; Response Time; GPS.

1 Introduction

Nowadays accelerates the progress of using of mobile devices and affiliated technologies dramatically and the number will be grow in the following years. It seems it will lead to the open wide application domains for PDAs (Personal Digital Assistants) and similar mobile devices that provide almost the same functionality as desktop application equivalents. The idea of such applications is based on current (and future) hi-tech devices with large scale (touch) display, large memory capabilities (with memory extension possibility) and wide spectrum of wireless network standard including bluetooth, Wi-Fi, GPS etc. Current example of device can be HTC Touch HD as a commercial device but there exists more industrial solutions.

Users of these portable devices use them all time in context of their life (e.g. moving, searching, alerting, scheduling, writing, etc.) or work. Context is relevant to the mobile user, because in a mobile environment the context is often very dynamic and the user interacts differently with the applications on his mobile device when the context is different [1]Users of these portable devices use them all time in context of their life (e.g. moving, searching, alerting, scheduling, writing, etc.). Context is relevant to the mobile user, because in a mobile environment the context is often very dynamic and the user interacts differently with the applications on his mobile device when the context is different [1].

K. Pentikousis et al. (Eds.): MONAMI 2009, LNICST 32, pp. 143–154, 2010.

Recent research of context-aware computing has been restricted to location-aware computing for mobile applications using a Wi-Fi network (LBS Location Based Services). The information about basic concept and technologies of user localization such as LBS, searching for Wi-Fi AP can be found in previous article [2]. On localization basis a special framework called PDPT (Predictive Data Push Technology) was implemented. This framework can improve a usage of large data artifacts of mobile devices [3]. Continuous user position information is used to determine a predictive user direction and position. Then is possibility to link data artifacts and prebuffer data by server to mobile device in consequence. When user arrives to predicted position and the position is equal to result by PDPT core, data artifacts are stored in PDA local memory (or the loading process finishing). Time for loaded data processing and display is shorter with using of prebuffered local data. User must not wait long time after the request.

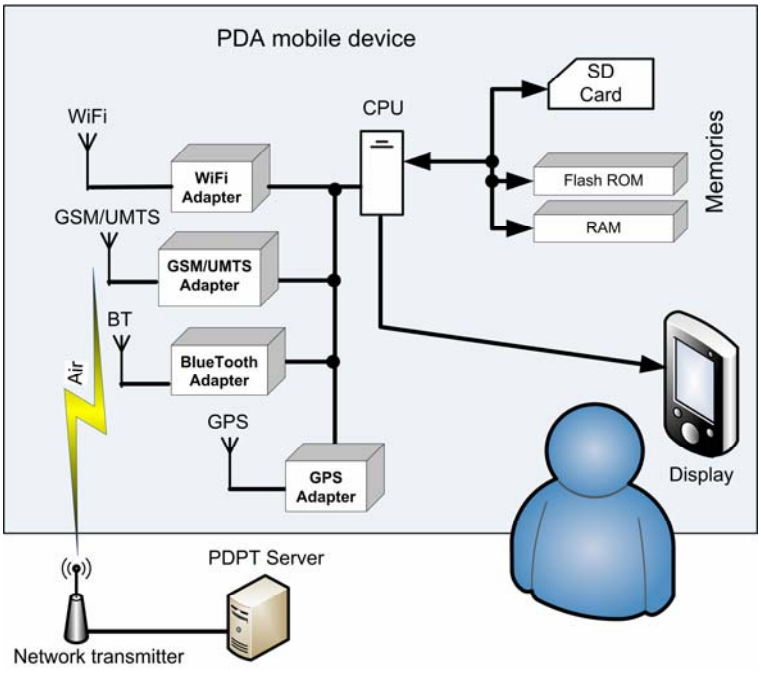


Fig. 1. Wireless networks and GPS sensor localization possibilities on mobile devices

In our case the WiFi was the starting point for framework implementation but the extension takes account of next wireless communication ways. For outdoor space there exists GSM/UTMS position utilities which can be implemented into application or GPS sensors often embedded in mobile devices either with Bluetooth wireless connection or SDIO wired GPS module etc. It is necessary to describe a position obtaining from wireless networks background in the beginning of next chapter to give a reader more information about these themes.

2 The PDPT Framework and PDPT Core

The general principle of my simple localization states that if a WiFi-enabled mobile device is close to such a stationary device – Access Point (AP) it may "ask" the provider's location position by setting up a WiFi connection. If position of the AP is known, the position of mobile device is within a range of this location provider. This range depends on type of WiFi AP. The Cisco APs are used in my test environment at Campus of Technical University of Ostrava. Measurements were performed on these APs to get signal strength (SS) characteristics and a combination of them called "super ideal characteristic" [5]. The computed equation for Super-Ideal characteristic is taken as basic equation for PDPT Core to compute the real distance from WiFi SS.

From this super ideal characteristic it is also evident the signal strength is present only to 30 meters of distance from base station. This small range is caused by using of Cisco APs. These APs has only 2 dB WiFi omnidirectional antenna. Granularity of location can be improved by triangulation of two or more visible WiFi APs. The PDA client will support the application in automatically retrieving location information from nearby location providers, and in interacting with the server. Naturally, this principle can be applied to other wireless technologies like Bluetooth, GSM or WiMAX. To let a mobile device determine its own position is needed to have a WiFi adapter still powered on. This fact provides a small limitation of use of mobile devices [4]. The test results with a possibly to use a PDA with turned on WiFi adapter for a period of about 5 hours.

2.1 Maximum User Response Time

PDPT framework is based on a model of location-aware enhancement, which we have used in created system. This technique is useful in framework to increase the real dataflow from wireless access point (server side) to PDA (client side). Primary dataflow is enlarged by data prebuffering. PDPT pushes the data from SQL database to clients PDA to be helpful when user comes at final location which was expected by PDPT Core. The benefit of PDPT consists in time delay reducing needed to display desired artifacts requested by a user from PDA. This delay may vary from a few seconds to number of minutes. Theoretical background and tests were needed to determine an average artifact size for which the PDPT technique is useful. First of all the maximum response time of an application (PDPT Client) for user was needed to be specified.

Nielsen [6] specified the maximum response time for an application to 10 seconds [7]. During this time the user was focused on the application and was willing to wait for an answer. The book is over 20 years old (published in 1994). We suppose the modern user of mobile devices is more impatient so the stated value of 10 second will be shorter. This is for me even better, because my framework is more usable. This time period (10 second) is used to calculate the maximum possible data size of a file transferred from server to client (during this period). If transfers speed wary from 80 to 160 kB/s the result file size wary from 800 to 1600 Kb [5].

The next step was an average artifact size definition. A network architecture building plan is used as sample database, which contained 100 files of average size of 470 kB. The client application can download during the 10 second period from 2 to 3

artifacts. The problem is the long time delay in displaying of artifacts in some original file types. It is needed to use only basic data formats, which can be displayed by PDA natively (bmp, jpg, wav, mpg, etc.) without any additional striking time consumption.

The final result of our 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.

2.2 From Data Collection to Localization

A first key step of the PDPT is a data collection phase. 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 WaveLAN NIC makes the signal strength (SS) available. SS is reported to units of dBm. Each time the broadcast packet is received the WaveLAN driver extracts the SS information from the WaveLAN firmware. Then it makes the information available to user-level applications via system calls.

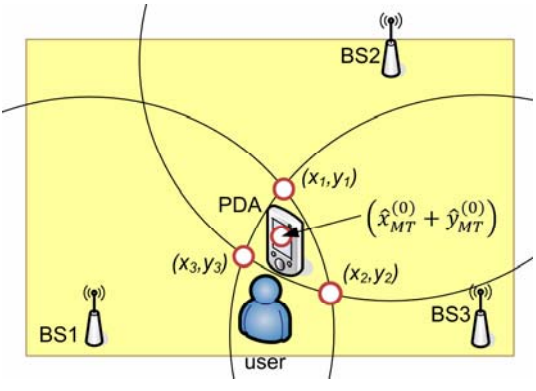


Fig. 2. Localization principle – triangulation

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. The typical range wary 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). The PDA client currently supports the application in automatically retrieving location information from nearby WiFi location providers, and in interacting with the PDPT server. Naturally, this principle can be applied to other wireless technologies like BT, GSM, UMTS or WiMAX. The application (locator) is implemented in C# language using the MS Visual Studio .NET with .NET Compact Framework and a special OpenNETCF library enhancement. Schema on figure [Fig. 2] describes a localization process. The mobile client gets the SS info of three BSs (Base Stations) with some inaccuracy. Circles around the BSs are crossed in red points on figure. The intersection red point (centre of three) is the best

computed location of mobile user. The user track is also computed from these measured SS intensity levels and stored in database for later use by PDPT Core. This idea is applicable in case of WiFi as well as BT and GSM networks.

In previous research, we focused only to use of WiFi networks while the other wireless possibilities remained without a proper notice. Now an enhancement of Locator component of PDPT framework [Fig. 4] is made to allow operate with BT and GSM networks.

BT

In BT network case, the position of BT APs must be known to allow the position determination. To collect BT APs position info in outdoor environment, the GPS can be used. For indoor area, the GIS (Geographic Information System) software with buildings map must be used to measure exact position of BT AP against to local environment. To manage with BT hardware of mobile device another library InTheHand 32Feet.NET is used.

GSM

GSM network is not local network but a cellular network. The problem is in position information of GSM BTSs (Base Transceiver Stations). The operator doesn't provide any such information. One of possible solutions is based on unofficial BTSs lists which can be found on internet. The lists are typically available in HTML, TXT or CSV formats. The medium rate for BTs with GPS position information is about 90 % of all BTs in European countries. In case of PDPT Framework, the list must be converted to PDPT server database – GSM_BTS table [Fig. 3].

In all three described cases of nearby BSs scanning, the data are saved to Locator Table in PDPT server DB [Fig. 3]. Data are processed from Locator Table throw the PDPT Core to Position Table. The processing techniques depend on selected wireless network. WiFi and BT network provide all visible APs nearby the user. From list of these APs is computed actual position (by triangulation [Fig. 2]).

Mobile devices with windows mobile operation system do not provide any GSM info to .NET Compact Framework. Even any special framework as in previous two cases is not known for me until now. Only possibility is in use of RIL (Radio Interface Layer) library. This library is divided into two separate components, a RIL Driver and a RIL Proxy. The RIL Driver processes radio commands and events. The RIL Proxy performs arbitration between multiple clients for access to the single RIL driver. When a module calls the RIL to get the signal strength, the function call immediately returns a response identifier. The RIL uses the function response callback to convey signal strength information to the module.

The GSM network provide only one BS info in each search cycle. This BS has the highest signal strength. The more BTSs info is collected by a several iteration cycles. During 10 cycles (per 10 seconds) the 4 BTS info is obtained on average.

The important info from BTSs is Signal Strength and Time Advance (TA). SS is refreshed every several seconds (in every scan) whereas TA is provided only during

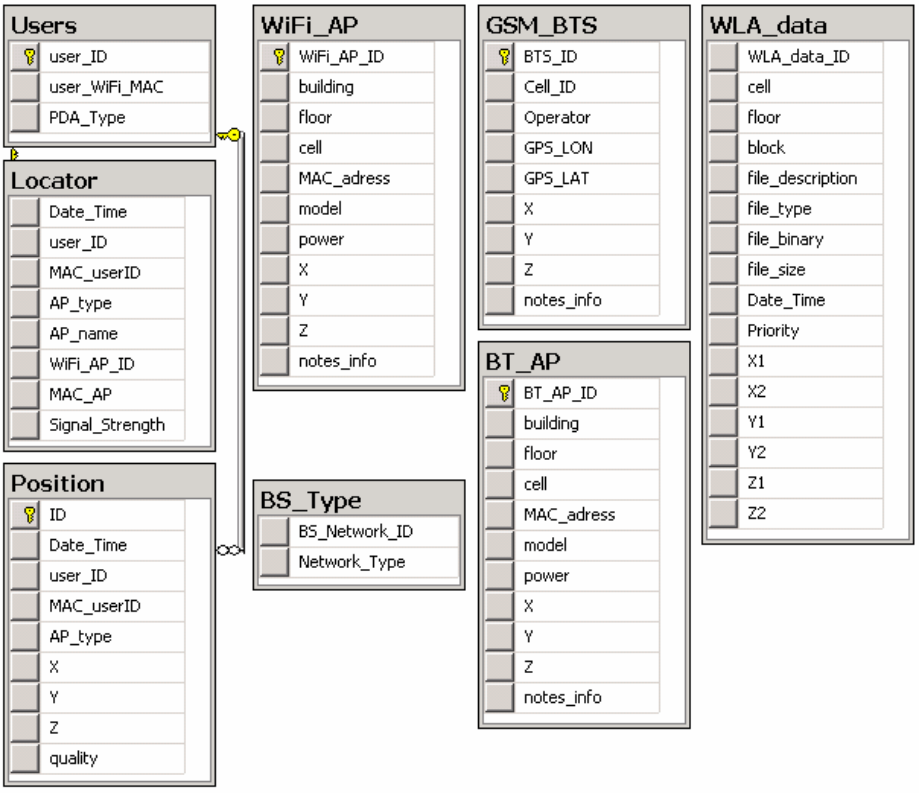


Fig. 3. PDPT server DB (Data Base) - New database architecture

some type of communication with selected BTS (e.g. request to talk, move to another area - Location Area Code (LAC)). The list of these BTSs with info is further processed as in previous case for WiFi and BT networks. Only change is in usage of TA if it is accessible.

GPS

Another possibility to get the user position in outdoor space is GPS (Global Positioning System) [8]. GPS provide a position by LONgitude and LATitude (X and Y). Only simple conversion is needed to transform a GPS coordinates to S-JTSK, which is used in PDPT Framework.

A GPS receiver calculates its position by precisely timing the signals sent by the GPS satellites above Earth. Each satellite continually transmits messages containing the time the message was sent, precise orbital information and the general system health and rough orbits of all GPS satellites. The receiver measures the transit time of each message and computes the distance to each satellite. Geometric trilateration is used to combine these distances with the location of the satellites to determine the receiver's location. GPS unit is able to calculate derived information as direction and

speed in many cases. In our case it can be useful for better prediction of user direction for more dynamic response. For more precise information about localization there is more than three satellites necessary. Therefore receivers use four or more satellites to solve for all three axis and time value, which is used to correct the receiver's clock. Most GPS applications use the computed location only and effectively hide the very accurately computed time, it is used in a specialized applications as time synchronization for outdoor transitional process measurement [13].

Although four satellites are required for normal operation, fewer apply in special cases. If one variable is already known (for example, a ship or plane may have known elevation), a receiver can determine its position using only three satellites. In PDPT framework there is no mandatory to use more than three satellites too.

For error analysis we have to calculate with more sources as a signal arrival time measurement (mainly used for localization calculation), athmospheric effects (ionospheres and tropospheres errors), multipath effects and so on.

Multipath effects is GPS signal affection by multipath issues, where the radio signals reflect off surrounding terrain; buildings, canyon walls, hard ground, etc. These delayed signals can cause inaccuracy. Long delay multipath effects is possible to discard more easily then short delay. Multiple effects are much less severe in moving objects. When the GPS antenna is moving, the false solutions using reflected signals quickly fail to converge and only the direct signals result in stable solutions. Because we consider to use GPS outdoor but within build-up area it is essential correct GPS receiver information.

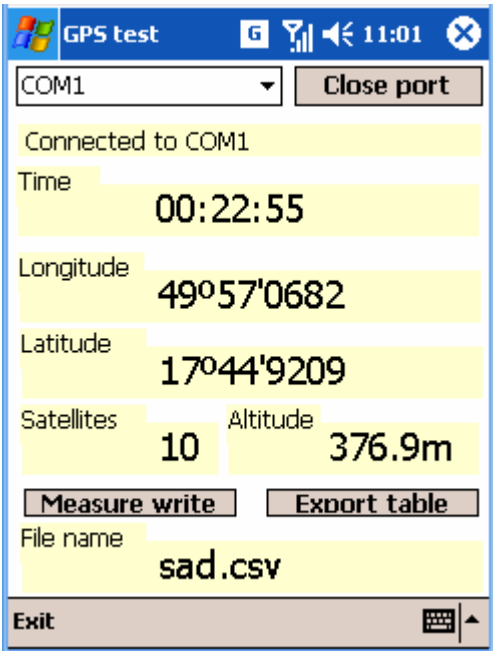


Fig. 4. GPS test application for PDA

Due free using of this technology by civilians there exists many mobile devices dedicated to a special areas, especially commercial applications in the tourist or car navigation. This means closed set of applications. But in new types of personal mobile devices we can find embedded GPS modules (or we can connect external GPS) and extend original PDPT framework with new capabilities of GPS.

Basic implementation of GPS software module for PDPT core was implemented with NMEA (National Marine Electronics Association) protocol decoder. By the $GPGGA (Global Positioning System Fix Data) sentence information string we get information about clock, latitude, longitude, number of satellites etc. This data can be stored in framework database and assigned to artifacts [Fig. 4]. A part of NMEA message received by used GPS module:

```
  $GPRMC,191843.000,A,4957.0673,N,01744.9146,E,0.00,220.7
0,010709,,,A*61
  $GPVTG,220.70,T,,M,0.00,N,0.0,K,A*0A
  $GPGGA,191844.000,4957.0673,N,01744.9146,E,1,09,1.0,381
.8,M,42.8,M,0.0,0000*76
  $GPRMC,191844.000,A,4957.0673,N,01744.9146,E,0.00,220.7
0,010709,,,A*66
```

In accordance with following table 1 we can obtain all required information.

Table 1. Table of data conversion by NMEA string to required values

Sequence	Example	Format and notes
1	191844.000	hhmmss.sss (UTC time in calculated position)
2	4957.0673	ddmm.mmmm (Latitude)
3	N	c (North/South indicator)
4	01744.9146	dddmm.mmmm (Longitude)
5	E	c (East/West indicator)
6	1	d (Quality indicator, 1 – successful, 0 – impossible to determine the position)
7	09	dd (Number of visible satellites)
8	1.0	d.d (Horizontal dilution of precision)
9	381.8	d.d (Antenna altitude above/below mean sea level (geoid))
10	M	c (meters – unit for antenna altitude)
11	42.8	d.d (Geoidal separation)
12	M	c (meters – unit for geoidal separation)
13	0.0	d.d (Age in seconds since last update from different reference station)
14	0000	dddd (Different reference station ID#)
15	*76	*xx (Control checksum)

For indoor environments there is possibility to use GPS receivers and repeaters instead of using WiFi network or its combination [Fig. 5].

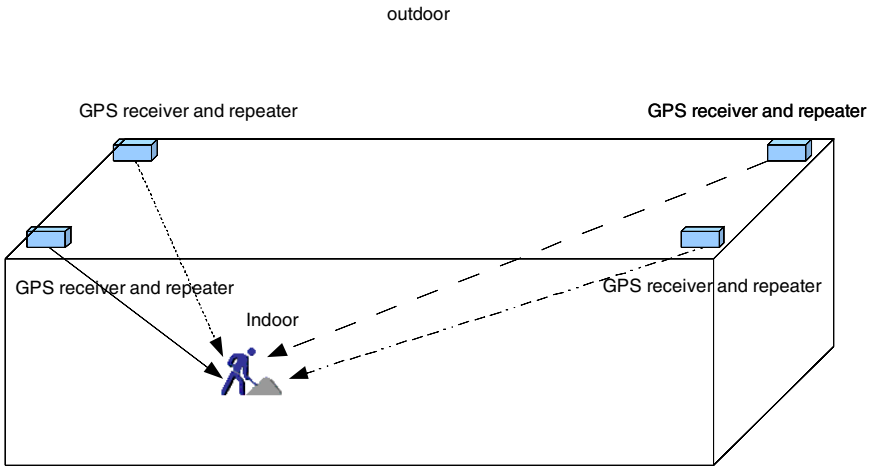


Fig. 5. Using GPS repeater indoor

2.3 The PDPT Framework Design

The PDPT framework design is based on the server-client architecture. The PDPT framework server is created as a web service to act as a bridge between MS SQL Server (other database server eventually) and PDPT PDA Clients [Fig. 6].

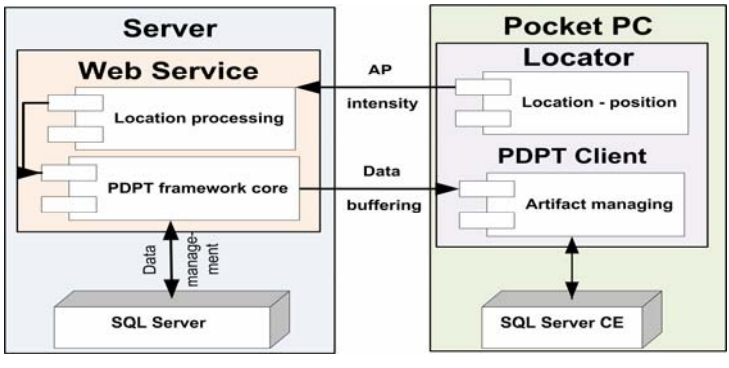


Fig. 6. PDPT architecture – UML design

Client PDA has location sensor component, which continuously sends the information about nearby AP's intensity to the PDPT Framework Core. This component processes the user's location information and it makes a decision to which part of MS SQL 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 PDA buffer imaginary image.

2.4 PDPT Core - Area Definition

The PDPT buffering and predictive PDPT buffering principle is relatively simple. Firstly the client must activate the PDPT on PDPT Client. This client creates a list of artifacts (PDA buffer image), which are contained in his mobile SQL Server CE database. Server create own list of artifacts (imaginary image of PDA buffer) based on area definition for actual user position and compare it with real PDA buffer image.

The area can be defined as an object where the user position is in the object centre. The cuboid is used as the object in present time for initial PDPT buffering. The PDPT Core will continue with comparing of both images. In case of some difference, the rest artifacts ale prebuffered to PDA buffer. When all artifacts for current user position are in PDA 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 user position it makes a new predictive enlarged imaginary image of PDA buffer. 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 and it will continue with buffering of artifacts until they are same [11].

2.5 PDPT Framework Data Artifact Management

The PDPT Server SQL database manages the information (artifacts) in the context of their location in building environment. This context information is same as location information about user track. The PDPT Core selecting the data to be copied from PDPT server to PDA client by context information (position info). Each database artifacts must be saved in database along the position information, to which it belongs. The new software application called "Data Artifacts Manager" was created to manage the artifacts in WLA database (localization oriented database). User can set the priority, location, and other metadata of the artifact. The Manager allows creating a new artifact from multimedia file (image, video, sound, etc.), and work with existing artifacts [5]. The needs of interface to operate with APs info arose out of the developing process of PDPT Framework. The enhancement of Artifact manager was created on that ground. Now the Artifact Manager contains a new tab "Base Stations Manager" to operate with APs or BSs of selected networks. This manager is connected directly to PDPT Server database, to tables WiFi_AP, BT_AP, GSM_BTS.

2.6 The PDPT Client Application

The PDPT Client application realizes thick client to the server side and an extension by PDPT and Locator modules. Figure [Fig. 7] shows three screenshots from the mobile client. The first one [Fig. 8a] shows the Locator module with selected GSM scanning. The info text box "Locator AP ret." Provide info about last founded GSM BTSs and number of recognized BTSs (BTSs with GPS position). In current case the 6 BTSs was founded and 5 of them was recognized by PDPT Framework. Figure [Fig. 8b] shows the classical view of the data artifact presentation from MS SQL CE database to user (in this case the image of Ethernet plan of the current area). The

PDPT tab [Fig. 8c] presents a way to tune the settings of PDPT Framework. The middle section shows the logging info about the prebuffering process. The right side means measure the time of one artifact loading ("part time") and full time of prebuffering in millisecond resolution. More screens and details of PDPT Client can be found in chapters 2.7 and 2.8 [5].

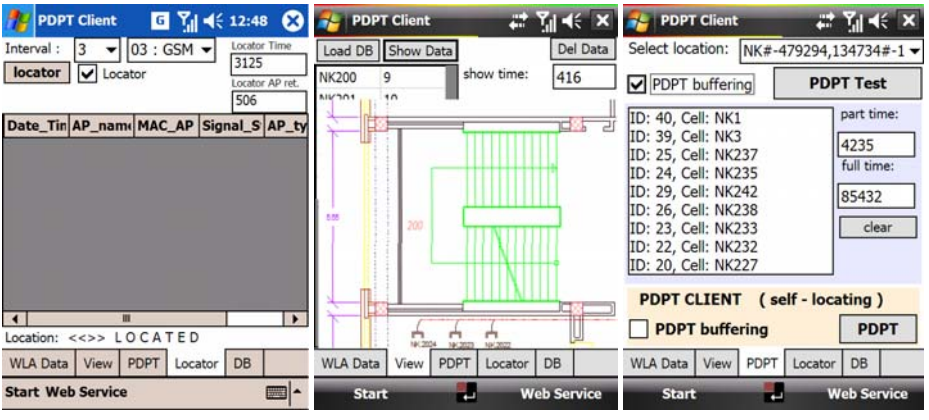


Fig. 7. PDPT Client – Left one figure 7a – Locator component with GSM scanning. Middle one figure 7b – View of normal client data representation. Right one figure 7c - The PDPT options screen allow to start and control the PDPT buffering.

3 Conclusions

This work is focused on the real usage of the developed PDPT framework on a wide range of wireless mobile devices and its main issue at increased data transfer rate. For testing purpose, few mobile devices were selected with different hardware and software capabilities. The high success rate found in the test data surpassed our expectations. This rate varies from 84 to 96 % [5].

The PDPT prebuffering techniques can improve the using of medium or large artifacts on wireless mobile devices connected to information systems. The localization part of PDPT framework is currently used in another project of biotelemetrical system for home care named Guardian to make a patient's life safer [12]. Another utilization of PDPT consists in use of others wireless networks like BT, GSM/UMTS, WiMAX, or in GPS. This idea can be used inside the information systems like botanical or zoological gardens where the GPS navigation can be used in outdoor. Some improvements of Locator module or Artifact Manager are described as well as improved architecture of PDPT server database. The larger area of PDPT utilization can improve importance of PDPT Framework in wireless mobile systems.

Acknowledgment. This work was supported by the Ministry of Education of the Czech Republic under Project 1M0567.

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, Boston, USA, 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. Krejcar, O.: PDPT Framework - Building Information System with Wireless Connected Mobile Devices. In: ICINCO 2006, 3rd International Conference on Informatics in Control, Automation and Robotics, Setubal, Portugal, August 01-05, pp. 162–167 (2006)
5. Krejcar, O., Cernohorsky, J.: New Possibilities of Intelligent Crisis Management by Large Multimedia Artifacts Prebuffering. In: Ulieru, M., Palensky, P., Doursat, R. (eds.) I.T. Revolutions 2008. LNICST, vol. 11, pp. 44–59. Springer, Heidelberg (2008)
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. In: Eurasip journal on applied signal processing. Hindawi publishing corp., New York (2006)
9. Arikan, E., Jenq, J.: Microsoft SQL Server interface for mobile devices. In: Proceedings of the 4th International Conference on Cybernetics and Information Technologies, Systems and Applications/5th Int Conf on Computing, Communications and Control Technologies, Orlando, FL, USA, July 12-15 (2007)
10. Jewett, M., Lasker, S., Swigart, S.: SQL server everywhere: Just another database? Developer focused from start to finish. DR DOBBS Journal 31(12) (2006)
11. Krejcar, O.: Utilization Possibilities of Area Definition in User Space for User-Centric Pervasive-Adaptive Systems. In: Hesselman, C., Giannelli, C. (eds.) Mobilware 2009. LNICST, vol. 12, pp. 124–130. Springer, Heidelberg (2009)
12. 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. 286–293. Springer, Heidelberg (2009)
13. Slanina, Z., Krejcar, O., Stambachr, J., Silber, P., Frischer, O.: Noninvasive Continuous Blood Pressure Measurement and GPS Position Monitoring of Patients. In: 2009 IEEE 70th Vehicular Technology Conference, Anchorage (2009)

Author Index